Draft: 12/17/19

Privacy Protections (D) Working Group
Austin, TX
December 8, 2019

The Privacy Protections (D) Working Group of the Market Regulation and Consumer Affairs (D) Committee met in Austin, TX, Dec. 8, 2019. The following Working Group members participated: Cynthia Amann, Chair (MO); Ron Kreiter, Vice Chair (OK); Theodore J. Patton (MN); Kendall Cotton (MT); Bob Harkins (NE); and Don Beatty (VA). Also participating were Ryan James and Suzanne Tipton (AR); Peg Brown (CO); Angela Dingus (OH); Brian Fordham (OR); Travis Jordan (SD); and Tracy Klausmeier (UT).

1. Heard Opening Remarks

Ms. Amann said this is the first meeting of the Working Group, as it was appointed by the Market Regulation and Consumer Affairs (D) Committee during its Oct. 1 conference call. She said the Working Group is in the process of building its membership, as well as forming distribution lists for interested regulators and interested parties. Ms. Amann asked those interested in joining the Working Group or being added to a distribution list to contact Lois Alexander (NAIC).

2. Heard a Presentation from NAIC Staff on Model #670, Model #672, GDPR, CCPA and State Data Privacy Legislation Chart

Ms. Amann said Jennifer McAdam (NAIC) would be providing an overview of the *Insurance Information and Privacy Protection Model Act* (#670), the *Privacy of Consumer Financial and Health Information Regulation* (#672), the European Union's (EU) General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and the research chart of State Data Privacy Legislation prepared by NAIC Legal Division staff.

Ms. McAdam said she would be discussing what is currently happening at the state level with data privacy laws, but she would like to first give a quick overview of the NAIC model laws already in existence that address consumer privacy. She clarified that data privacy is related to how data is collected and used by businesses; data security is related to how data is stored and protected.

Ms. McAdam said she brought this up because the two are often conflated and—to make things more confusing—there are some laws that address both, like the GDPR, for example. She said an example of a data privacy law would be the CCPA. Ms. McAdam said this law governs how businesses collect and use consumer data; the rights consumers have so they know how that data is being used; the consumer's right to challenge the accuracy of the data; and, if is being used, how it is being used. As such, these laws are focused on consumer protection and consumer rights.

She said an example of a data security law would be the *Insurance Data Security Law* (#668), which governs how businesses protect the data once it has been collected and what the businesses need to do in the event the company's protections of that data fail during a data breach or cybersecurity event. Ms. McAdam said these laws are focused on business obligations, although such data security laws can have an impact on consumer protection, as well.

Ms. McAdam said the NAIC has three model laws governing data privacy: 1) The *Health Information Privacy Model Act* (#55); 2) Model #670; and 3) Model #672. She said because historical context is helpful, the first of these was Model #670, which was adopted in 1980. However, Ms. McAdam said the federal Fair Credit Reporting Act (FCRA) was enacted in 1970, and it addresses the fairness, accuracy and privacy of the personal information contained in the files of the consumer reporting agencies. Then, she said the Federal Privacy Act was enacted in 1974, and it governs the collection, maintenance, use and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. So, Ms. McAdam said the NAIC began drafting Model #670 after the two federal laws were in already in place.

Ms. McAdam said Model #670 sets standards for the collection, use and disclosure of information gathered in connection with insurance transactions; it addresses how information is collected by insurance institutions, agents and insurance support organizations (ISOs). She also said the model balances the need for information by those conducting the business of insurance and the public's need for fairness. Ms. McAdam said it establishes a regulatory mechanism to enable consumers to ascertain

what information is being, or has been, collected about them and to have access to such information so they can verify or dispute its accuracy. She said it limits the disclosure of information collected in connection with insurance transactions, and it enables insurance applicants and policyholders to find out the reasons for any adverse underwriting decision. Ms. McAdam said the model does this by requiring insurers to provide notice that alerts the individual of the insurer's information practices and it gives consumers the right to request that an insurer: 1) give access to recorded personal information; 2) disclose the identity of the third parties to whom the insurance disclosed the information; 3) provide the source of the collected information; 4) correct and amend the collected information; 5) amend the personal information; and 6) delete the collected personal information.

Ms. McAdam said the definition of "personal information" is different from that of the protected information found in most of the data security or data breach notification laws. She said those laws tend to specifically enumerate the categories of data that must be protected. Ms. McAdam said in this model "personal information" means any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health or any other personal characteristics.

In 1998, following enactment of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), the NAIC adopted Model #55, which sets standards to protect health information from unauthorized collection, use and disclosure by requiring carriers to establish procedures for the treatment of all health information. Ms. McAdam said Model #55 requires carriers to: 1) create policies, standards and procedures governing health information; 2) notify consumers of those policies, standards and procedures; 3) establish consumers' right to access their personal health information (PHI); 4) establish consumers' right to amend their PHI; 5) provide a list of disclosures of PHI; and 6) obtain authorization for the collection, use or disclosure of PHI (with exceptions).

Following enactment of HIPAA at the federal level, Ms. McAdam said the federal Gramm-Leach-Bliley Act (GLBA) was enacted in 1999. She said GLBA imposes privacy and security standards on financial institutions and directs state insurance commissioners to adopt certain data privacy and data security regulations. She said that is when the NAIC adopted both Model #672 and the *Standards for Safeguarding Customer Information Model Regulation* (#673). Ms. McAdam said Model #672 is about consumer privacy, and Model #673 is about data security and was used as the basis for drafting Model #668.

Ms. McAdam said this Working Group will be addressing data privacy; it will not be addressing data security. She also said Model #672: 1) requires that insurers provide notice to consumers about its privacy policies and practices; 2) describes the conditions under which a licensee may disclose nonpublic PHI and nonpublic personal financial information about individuals to affiliates and nonaffiliated third parties; and 3) provides methods for individuals to prevent a licensee from disclosing that information ("opt out" for financial info and "opt in" for health information). Ms. McAdam said this model is intended to be enforced via the state's Unfair Trade Practices Act. She said the provisions governing protection of health information were taken directly from Model #55, as well as the health information privacy regulations promulgated by the U.S. Department of Health and Human Services (HHS) pursuant to HIPAA. Ms. McAdam said the provisions governing the protection of financial information are based on privacy regulations promulgated by federal banking agencies.

Ms. McAdam said the key difference between the treatment of financial information and health information is that insurers must give consumers the right to "opt out" of the disclosure or sharing of their financial information, but insurers must get explicit authorization prior to sharing health information (which is considered "opt in").

Ms. McAdam said the protected information under Model #672 is "health information" and "personally identifiable financial information." She said 17 states have adopted Model #670 and every state has adopted a version of Model #672, although 19 states have only adopted the provision regarding financial information and not the provision regarding health information. Ms. McAdam said NAIC guidance on data privacy includes the privacy standard used in market conduct examinations. She said standards 10 through 16 address how companies are to handle data privacy pursuant to Model #670, Model #672, Model #55 and any other data privacy laws to which companies are subject.

Ms. McAdam said there are generally applicable data privacy laws that apply to all businesses; not just to the insurance sector. She said data privacy started getting more attention when the GDPR became effective in May 2018. Ms. McAdam said although it is an EU law, it affects many U.S. companies if they collect data from citizens of the EU over the internet. She said the GDPR

requires companies to obtain explicit consent from consumers to collect their data ("opt in") with an explanation of how the data will be used and it contains standards for safeguarding the data.

Ms. McAdam said California became the first U.S. state to adopt an "omnibus" privacy law, which imposes broad obligations on businesses to provide consumers with transparency and control of their personal data. She said the CCPA was signed into law last summer, was amended last fall and becomes effective in 2020. Ms. McAdam said the CCPA gives consumers the right to request that a business:

- Disclose (a) the categories and specific pieces of personal information collected; (b) categories of sources the information was collected from; (c) the business purpose for collecting the information; and (d) the categories of third parties with whom the information is shared, and the specific pieces of personal information that was shared.
- Delete any personal information.
- Provide the right to opt-out of their information being disclosed to third parties, with separate opt-in requirements for minors.
- Provide the right to not be discriminated against for exercising rights.

Ms. McAdam said the CCPA is enforced by the state attorney general and there is a full exemption for protected health information governed by HIPAA and a partial exemption for information subject to the GLBA; if the information subject to GLBA is breached, the consumer can pursue a private civil action against the company.

Ms. McAdam said some states introduced similar data privacy laws to the CCPA that were generally applicable. She said amendments to the CCPA were introduced during the 2019 legislative session, but none of them specifically affect insurers; the full HIPAA exemption and partial GLBA exemption remain in place.

Ms. McAdam said, in 2019, 24 states had considered some type of data privacy legislation but only three states enacted laws: 1) Illinois, which bans insurers from using genetic testing information to set health or accident rates; 2) Maine, which bans internet providers from selling personal information without consent; and 3) Nevada, which requires businesses to allow consumers to opt out of any sale of their personal information and has exemptions for entities subject to the GLBA and HIPAA.

Ms. McAdam said five states passed bills establishing task forces to study the issue of data privacy by reviewing laws in other states and making recommendations for what would be appropriate privacy standards: Connecticut; Hawaii; Louisiana; North Dakota; and Texas. She said there are some states with legislation still pending and some that will carryover to 2020. For example, in New York, there was a bill pending that would go further than the CCPA and would establish a fiduciary duty for companies to act in the consumer's best interest regarding their personal information; however, it did not make it out of committee but will be considered in 2020.

Ms. McAdam said a comparison of business obligations and consumer rights related to data privacy under both the CCPA and Model #670 shows the following similarities in those requirements.

CCPA	**Model #670**
Consumer right to request that a business:	Individual right to request that an insurer:
• Disclose the categories and specific pieces of personal information collected	• Disclose types of personal information collected
• Disclose categories of sources	• Disclose sources of the collected information
• Disclose business purpose for collecting the information	• Disclose purpose for collecting the information
• Disclose categories of third parties with whom the information is shared, and specific pieces of personal information shared	• Disclose identity of the third parties to whom information is disclosed
• Right to access, correct, delete	• Right to access, correct, delete

Ms. McAdam said NAIC Legal Division staff created several legal research charts that were posted to the Privacy Protections (D) Working Group page on the NAIC website. She said one chart lists general state data privacy laws that are applicable to all businesses and are not specific to insurers. She also said the chart lists the entity responsible for enforcing the law; what exemptions there are, if any; whether it is "opt-in" or "opt-out"; and what consumer notice requirements are required.

Ms. McAdam said the Working Group will want to address insurance-specific data privacy issues while making sure that any new requirements work with already-existing laws. She said it will be important to consider the following questions going forward: 1) what types of data collection, sharing and usage are specific to insurers; 2) what privacy risks affect insurance consumers; 3) where the gaps are in federal and state law; 4) what obligations insurers should have to consumers; and 5) what rights consumers should have to control their personal information.

Ms. Amann said Ms. McAdam will continue to provide any legal assistance the Working Group needs throughout the process. She then asked if any Working Group members had any comments.

Mr. Cotton said he is concerned about the consumer data that insurers already are presenting to Montana in rate filings. He said rate filings have ballooned up to thousands of pages of different data points on consumers. Mr. Cotton said Montana has seen an increased reliance on third-party risk scores that aggregate consumer information in order to make determinations and conclusions about that information. He said insurers have a responsibility to make sure that the third parties used are following state laws and complying with the state's standards for accuracy and fairness. Besides providing disclosure of those third parties when consumers request it, Mr. Cotton said insurers are required to report how the information was gathered; where it was drawn from (e.g., web traffic, geolocation data, social media, etc.); and why the company thinks it needs to use these particular data points as the possibilities available to insurers are endless.

3. Discussed the Draft Briefing Document, "Privacy Protections (D) Working Group Workplan"

Ms. Amann said the Working Group will need to stay on track in order to accomplish its charges by the deadline. She said the Working Group's proposed charges will be considered for adoption by the Market Regulation and Consumer Affairs (D) Committee during its Dec. 9 meeting.

Ms. Amann said this Working Group will work closely with the other working groups in this arena—the Artificial Intelligence (EX) Working Group, the Accelerated Underwriting (A) Working Group, etc.—as each has its unique set of issues that nevertheless require coordination.

4. Heard Comments from Interested Parties

   a. NAMIC

Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) urged regulators to consider the impact of California's law and the likely passage in 2020 of other state laws that may differ dramatically from it. Ms. Paolino asked that regulators analyze and identify any gaps that might need insurance-specific language. She said regulators could then determine the most appropriate vehicle to deliver that solution; i.e., whether to amend existing models or to draft new models.

Ms. Paolino urged policymakers to consider several important concepts:

- Workability – Allowing for various exemptions for operational and other reasons that acknowledge vital business purposes for insurers to collect, use, and disclose information. For example, she said Article IV of Model #672 was developed to implement the GLBA; it appears instructive on types of operational functions to preserve and facilitate. Ms. Paolino said it may also be useful to review the exceptions imbedded into Section 13 of the 1982 version of Model #672. She said clear and well-crafted provisions accounting for the GLBA and the FCRA would be important in any broader business legislation regulators may see.
- Exclusivity – Avoiding dual regulation so insurers are not simultaneously subject to potentially inconsistent or conflicting interpretations by more than one regulator.
- Clarity – Asking that care be taken to consider how best to dovetail with existing model laws/regulations; consulting other resources and educating legislators on how privacy bill language impacts the insurance industry, including the legal requirements to retain and use certain data, as well as data mandates.
- Effective Date – Allowing advance time (like the two to five years that was afforded under the GDPR) for insurers to be ready for implementation, to avoid having revisions like the CCPA and the GDPR. She also suggested that a roll-out period with different dates for different provisions would be a more measured approach within that time frame to undertake such a significant endeavor.

b. APCIA

Angela Gleason (American Property Casualty Insurance Association—APCIA) agreed with NAMIC's assessment with regard to the implementation time frame, the initial survey request and the complex array of laws that state legislatures may pass during the December to January time frame that could put insurers in the position of complying with omnibus privacy bills in one state and industry-specific bills in another state. She said it could bring about some difficult compliance issues, which could reduce, rather than enhance, existing consumer protections and generate significant operational challenges. She said state insurance departments could play an important role in these legislative conversations based on their experience with insurance-specific privacy laws that are consistent with regulators' objectives to protect consumers and ensure insurer solvency.

Ms. Gleason said insurers are scrambling to be ready for the effective date of the CCPA that takes effect Jan. 1, 2020 and gives consumers more ability to control what information is shared about them.

c. ACLI

Kate Kiernan (American Council of Life Insurers—ACLI) said the regulatory environment is evolving. She said existing privacy laws have been on the books since the mid-1980s and late 1990s with little change, which reflects well on the stability of the insurance regulatory structure. However, she said that advances in technology and changes in the insurance industry have resulted in rendering some of the existing financial services privacy laws as being somewhat outdated.

Ms. Kiernan asked the Working Group to think about how ride- and home-sharing services, such as Uber and Airbnb, have disrupted the livery and hospitality industries. She asked the Working Group to look at the big picture to ensure that the insurance industry does not encounter a complete change of its industry like that which happened in the hospitality and livery industry.

Ms. Kiernan said even though policyholders might welcome stiffer regulation initially, stiffer regulation could unintentionally harm the companies that serve those consumers. She said caution is warranted when considering additional regulation to ensure a level playing field with how all other companies are collecting personal information, so insurance companies are not disadvantaged when compared to the technology sector.

Ms. Kiernan said consistency across states and business types is necessary so insurers will not be required to meet industry-specific privacy rules, while companies like Amazon, Google and the Insure Techs have different rules to meet.

Ms. Kiernan asked the Working Group to consider the following questions:

- How do you envision the current financial services privacy regulatory system meshing with new comprehensive laws such as the CCPA?
- How will financial services companies be able to compete with technology companies with differing rules on the use of personal information?
- How can we provide control and equal protections to all consumers regarding their personal information no matter where they live or with whom they are doing business? In other words, provide consumers with legal transparency and the same level enforceable rights?
- How can we develop a regime that is robust and supports growth and innovation?

Ms. Kiernan said to put these questions another way:

- How do we avoid consumer confusion over this already complex issue?
- How do we avoid the obstruction of the flow of data and impediments to interstate commerce?
- How do we prevent the distortion of competition (tech versus retail versus financial services)?

In conclusion, Ms. Kiernan said technology is transforming both social norms and business capabilities. The internet is universal, and information is global. Consumers and businesses need standards that are coherent, and that provide a common understanding of privacy protections. Ms. Kiernan said policymakers should avoid creation of a system that would provide differing consumer rights; differing levels of protections; fragmented implementation of consumer protections; and legal uncertainty.

Ms. Kiernan said this complex issue warrants a comprehensive review and she looks forward to working with the Working Group as it moves forward. Ms. Kiernan said she would like to align her comments with the recently submitted observations of NAMIC and the APCIA because she agrees with the thoughtful comments regarding specific issues and challenges that her sister national trade associations raised in their remarks.

d. CEJ

Birny Birnbaum (Center for Economic Justice—CEJ) said Model #670 addresses "personal information," while Model #672 addresses "nonpublic personal financial information and nonpublic personal health information." He said both models discuss "consumer reports" and "consumer reporting agencies," as defined by the FCRA.

Mr. Birnbaum asked the Working Group to consider:

- Data vendors are scraping personal consumer information from public sources to produce consumer profiles, scores and other tools for insurers. The data vendor products, while assembled from public information, raise concerns over consumers' digital rights and privacy.
- Many data vendors and many types of personal consumer information are not subject to FCRA consumer protections. In turn, many of the types of data and algorithms (essentially, a consumer report) used by insurers are not subject to either FCRA consumer protections or the NAIC model law/regulation protections.
- It is unclear if the NAIC models cover the new types of data being generated by consumers as part of, or related to, insurance transactions. For example, consumers are producing large volumes of data through telematics programs—from devices collecting personal consumer data in the vehicle or home or wearable devices.
- There are a lot of organizations working on consumer digital rights. He asked the Working Group to solicit input and presentations at Working Group meetings from, among others, the Center for Digital Democracy, the Electronic Privacy Information Center, the Electronic Frontier Foundation, the Public Knowledge-Privacy Rights Clearinghouse, the Public Citizen, the U.S. Public Interest Research Group and the World Privacy Forum. In addition, Mr. Birnbaum said there are several organizations active on digital rights in the EU that are familiar with the GDPR and whose perspectives would help the Working Group.
- He asked that if consumer disclosures are to be used, that the disclosure should be a compliance or enforcement tool that would be created using consumer focus testing and established best practices for the creation of such consumer disclosures.

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

W:\National Meetings\2019\Fall\Cmte\D\Privacy Protections\Privacyprot_12min_JMM121719.Docx

