Draft Pending Adoption

Attachment XX
Market Regulation and Consumer Protection (D) Committee
8/11/20

Draft: 8/18/20

Privacy Protections (D) Working Group
Virtual Summer National Meeting
July 30, 2020

The Privacy Protections (D) Working Group of the Market Regulation and Consumer Affairs (D) Committee met via conference call July 30, 2020. The following Working Group members participated: Cynthia Amann, Chair, and Marjorie Thompson (MO); Ron Kreiter, Vice Chair (OK); Damon Diederich (CA); Erica Weyhenmeyer (IL); LeAnn Crowe and Brenda Johnson (KS): T.J. Patton and Paul Hanson (MN); Kendall Cotton (MT); Chris Aufenthie and Anders Odegard (ND); Martin Swanson (NE); Tasha Sizemore (OR); Gary Jones (PA); and Don Beatty (VA). Also participating were: Jimmy Harris and Crystal Phelps (AR); Damion Hughes (CO); Evangelina Brooks (FL); Doug Ommen (IA); Kristen Finau and Michele Mackenzie (ID); Kate Kixmiller (IN); Peggy Willard-Ross (NV); Don Layson (OH); Landon Hubbart (OK); Ignatius Wheeler and Carole Cearley (TX); John Haworth (WA); and Barbara Belling (WI).

1. Adopted its May 5 Minutes

Ms. Amann said the Working Group met May 5 and took the following action: 1) adopted its Feb. 19 minutes; 2) heard an update on state and federal privacy legislation; and 3) discussed comments received on the *NAIC Insurance Information and Privacy Protection Model Act* (#670).

Mr. Kreiter made a motion, seconded by Ms. Weyhenmeyer, to adopt the Working Group's May 5 minutes (Attachment ____-A). The motion passed unanimously.

2. Received an Update on State and Federal Privacy Legislation

Jennifer McAdam (NAIC) said a review of the laws about consumer privacy start with data privacy, addressing how data is collected and used by businesses, while data security addresses how data is stored and protected. Ms. McAdam said the NAIC has three model laws governing data privacy: 1) *Health Information Privacy Model Act* (#55); 2) *NAIC Insurance Information and Privacy Protection Model Act* (#670); and 3) *Privacy of Consumer Financial and Health Information Regulation* (#672).

Ms. McAdam said Model #670 was adopted in 1980 to set standards for the collection, use and disclosure of information gathered in connection with insurance transactions. She said it has been enacted by 17 states and addresses how information is collected by insurance institutions, agents and insurance support organizations (ISOs). She said Model #670 balances the need for information by those conducting the business of insurance and the public's need for fairness; 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; limits the disclosure of information collected in connection with insurance transactions; and enables insurance applicants and policyholders to find out the reasons for any adverse underwriting decision. She said Model #670 does this by requiring insurers to provide notice that alerts the individual of the insurer's information practices and giving 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 insurer 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 federal Fair Credit Reporting Act (FCRA) was enacted in 1970 to address the fairness, accuracy and privacy of the personal information contained in the files of the consumer reporting agencies and the Federal Privacy Act was enacted in 1974 to govern the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.

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

Draft Pending Adoption

Ms. McAdam said the federal Gramm-Leach-Bliley Act (GLBA), enacted in 1999, imposed privacy and security standards on financial institutions and directed state insurance commissioners to adopt certain data privacy and data security regulations.

Ms. McAdam said the NAIC adopted Model #672 in 1999 to: 1) require insurers to provide notice to consumers about their privacy policies and practices; 2) describe the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal financial information about individuals to affiliates and nonaffiliated third parties; and 3) provide methods for individuals to prevent a licensee from disclosing that information with "opt out" for financial information and "opt in" for health information. She said Model #672 is intended to be enforced via states' Unfair Trade Practices Act. She said the provisions governing protection of health information were taken directly from Model #55 and the health information privacy regulations promulgated by U.S. Department of Health and Human Services (HHS) pursuant to HIPAA. She also said the provisions governing 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"). She said every state has adopted a version of Model #672.

Ms. McAdam said generally applicable data privacy laws, such as the European Union's General Data Protection Regulation (GDPR), are not insurer-specific and require companies to obtain explicit consent from consumers to collect their data ("opt in") with an explanation of how the data will be used. The GDPR also contains standards for safeguarding the data. She said the California Consumer Privacy Act (CCPA) became effective this year and gives consumers the right to request that a business: 1) disclose the categories and specific pieces of personal information collected, the categories of sources the information was collected from, the business purpose for collecting the information, the categories of third parties with whom the information is shared, and the specific pieces of personal information that was shared; 2) delete any personal information; and 3) give consumers the right to opt-out of their information being disclosed to third parties. It also prevents companies from discriminating against consumers who exercise their rights under the law and provides a full exemption for PHI governed by HIPAA and a partial exemption for information subject to the GLBA. However, if the information subject to the GLBA is breached, the consumer can pursue a private civil action against the company.

Ms. McAdam said there has not been much change in the state legislative arena. She said in 2019, 24 states considered some type of data privacy legislation but only three states enacted laws: Illinois; Maine; and Nevada. She said five states—Connecticut, Hawaii, Louisiana, North Dakota and Texas—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. Ms. McAdam said more than 15 states introduced data privacy legislation in 2020 but none of them has been passed. She said many of these bills were fairly comprehensive and similar to the CCPA.

Brooke Stringer (NAIC) said there has not been a lot of activity on the federal level since the last Working Group call. She said for today's federal update, she would provide: 1) an overview of a new federal data privacy bill from U.S. Sen. Sherrod Brown (D-OH), who serves as the ranking Democrat on the U.S. Senate Committee on Banking, Housing and Urban Affairs; 2) briefly recap the four other bills previously proposed; and 3) conclude with a mention of some COVID-19 data privacy bills that have been introduced.

Ms. Stringer said, as she had mentioned before, the key issues for congressional debate focus on trade-offs regarding the extent of preemption, private rights of action, and the stringency of the standard. She said the most recent *draft* bill is from Sen. Brown, the "Data Accountability and Transparency Act," which: 1) establishes a new federal agency to protect individuals' privacy that would have rulemaking, supervisory and enforcement authority, the ability to issue civil penalties for violations of the act, and an Office of Civil Rights to protect individuals from discrimination; 2) prohibits the use of personal data to discriminate in housing, employment, credit, insurance and public accommodations; 3) requires anyone using decision-making algorithms to provide accountability reports to the new federal agency; 4) does not preempt more protective state laws and provides for enforcement by the state attorneys general; 5) bans the use of facial recognition technology, as well as the collection, usage or sharing of any of that personal data; 6) and contains a private right of action.

Draft Pending Adoption

Ms. Stringer said, as a recap, she would mention some of the other legislative proposals the Working Group has discussed previously:

- U.S. Senate Committee on Commerce, Science and Transportation Chairman Roger Wicker's (R-MS) draft bill, the "Consumer Data Privacy Act," that proposes stringent data privacy standards and preempts all state data privacy and security laws. She said it has a GLBA carveout, which should protect some state data privacy laws. A technical fix was proposed to clarify that the bill preserves state laws and regulations developed in accordance with the GLBA. She said it also provides standards for transparency; consumer rights to access, correct, delete their data; requires affirmative consent before collecting, processing or transferring data; calls for a Federal Trade Commission (FTC) study examining the use of algorithms that may violate anti-discrimination laws; and provides enforcement of the bill's provisions by the FTC and state attorneys general.
- U.S. Sen. Maria Cantwell (D-WA), the ranking Democrat on the U.S. Senate Committee on Commerce, Science and Transportation, introduced the "Consumer Online Privacy Rights Act (S. 2968)," which contains standards similar to the Wicker proposal, but would establish a preemptive floor and allow for a private right of action.
- The U.S. House of Representatives' Committee on Energy and Commerce's bipartisan draft proposal would provide the FTC with significant rulemaking authority to implement standards. Ms. Stringer said the questions surrounding preemption and private right of action remain subject to negotiation. NAIC staff have had discussions with congressional staff about the NAIC's privacy models and efforts to update them.
- U.S. Sen. Jerry Moran's (R-KS) "Consumer Data Privacy and Security Act (S. 3456)" has concepts like the Wicker and Cantwell proposals. Ms. Stringer said it preempts state data privacy and security laws but would not supersede state laws that address financial information held by financial institutions defined in Title V of the GLBA (the GLBA covers persons providing insurance).

Ms. Stringer said, in addition to comprehensive data privacy proposals, she wanted to mention that there have been several bills introduced that specifically address COVID-19 data privacy. She said the following proposals would put temporary rules in place regarding the collection, processing and transfer of data used to combat the spread of COVID-19: 1) Chairman Wicker's "COVID-19 Consumer Data Protection Act (S. 3663)," which requires covered entities to obtain affirmative consent before collecting, processing or transferring an individual's personally identifiable information for the purpose of contact tracing with respect to COVID-19. It preempts state laws and has no private right of action; and 2) the "Public Health Emergency Privacy Act (S. 3749/H.R. 6866)" by U.S. Sen. Richard Blumenthal (D-CT) and U.S. Rep. Anna Eshoo (D-CA) requires opt-in consent and data minimization, has a private right of action and does not preempt state laws. Ms. Stringer noted that the U.S. Congress is struggling with passing the next COVID-19 relief bill, so it is unlikely there will be any immediate action on the aforementioned COVID-19 bills.

Ms. Stringer said, in terms of future actions on comprehensive data privacy legislation, given the pandemic, the fact that it is an election year and with the general partisan discord, she said it is unlikely there will be any major congressional movement before the November elections. She also said it may be the next U.S. Congress that ultimately tackles these issues.

3. Heard a Presentation that Included a Comparative Analysis and Comments Received July 24

Chris Peterson (Arbor Strategies, LLC), representing America's Health Insurance Plans (AHIP), the Blue Cross and Blue Shield Association (BCBSA) and the Coalition (an organization that includes Aetna, Anthem, Cigna, Health Care Service Corporation and UnitedHealthcare), said phase one of any gap analysis by the Working Group should be a side-by-side comparison. He said the health insurance industry he represents has submitted a side-by-side comparison as a first step in completing a gap analysis.

Mr. Peterson said this analysis compares various approaches to regulating privacy, which the NAIC would use to determine whether those gaps are significant and/or relevant to state insurance regulators, insurance consumers and the insurance industry. He said before conducting this final analysis or final phase of its gap analysis, the Working Group should establish a base for conducting comparative analysis, as well as determine parameters for conducting analysis and evaluating gaps. Mr. Peterson agreed with the Working Group that the most logical approach would be to use Model #672 because it reflects the NAIC's most current thinking on privacy regulation; it is universally adopted at the state level; and other NAIC models have previously been rejected as base models by the Working Group during its meetings. He said the parameters for conducting the analysis should be focused solely on insurance licensees, insurance practices and insurance transactions.

Draft Pending Adoption

Mr. Peterson said the analysis should not regulate business in general, non-insurance practices or non-insurance transactions. He said any gaps that are identified should only be filled by concepts that have consensus support at the state level (also known as the "Walter Bell Rule") and that the resulting model should be aligned with existing federal laws. Mr. Peterson provided a comparison of the following aspects of Model #672, HIPAA, Model #670, the CCPA and the GDPR: 1) applicability; 2) definition of "covered or personal information"; 3) privacy notices; 4) opt-in/opt-out rights; and 5) consumer rights.

Lauren Choi (BCBSA) said while she applauds the Working Group's efforts, she reiterated that updates made to any privacy model would require a deliberative and considered approach based on facts and policy. She said state insurance regulators and the industry together can move forward only if the current landscape of existing federal law in the privacy arena is understood. To assist the Working Group in its efforts, she said the BCBSA and the Coalition has conducted a gap analysis of the specific privacy requirements with which certain insurance licensees must comply, including HIPAA, the CCPA, Model #670, Model #672 and the GDPR.

Ms. Choi said she hopes this material will be helpful to the Working Group to increase the Working Group's understanding of the existing consumer protections under current regimes. She said the BCBSA and the Coalition have learned that the Working Group has determined it is more beneficial for to focus its efforts on Model #672 instead of Model #670. Ms. Choi said the BCBSA fully supports and appreciates this decision, because, as it compares to Model #670, the newer Model #672 was developed to improve on Model #670; is much more reflective of current regulatory thinking and attitudes; and has been far more widely accepted in the states. She said Model #672 is a viable foundation for the Working Group to review and to determine what changes, if any, are needed to effectively protect consumer interests in the insurance arena.

4. Discussed Plans to Begin a Gap Analysis Discussion by Working Group Members, Interested State Insurance Regulators and Interested Parties Using Model #672 as a Baseline Model

Ms. Amann said the Working Group will begin its gap analysis discussion using Model #672 as a baseline. She said the plan is to break the analysis discussion down into three separate areas: 1) consumer issues; 2) industry obligations; and 3) regulatory enforcement. She said to help the Working Group visualize each of the topics to be discussed, two comparison charts created by Ms. McAdam indicating how Model #670, Model #672, the GLBA, HIPAA and the CCPA address them were posted to the Working Group's page on the NAIC website prior to this meeting. She said the Working Group would start its discussion at its next meeting with consumer issues such as disclosures, notifications, portability, opt-in/opt-out, changes, deletions, etc.

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

W:\National Meetings\2020\Summer\Cmte\D\Privacy Protections\Privacyprot_08min.Docx

