Draft Pending Adoption

Draft: 8/28/24

Privacy Protections (H) Working Group
Chicago, Illinois
August 14, 2024

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Chicago, IL, Aug. 14, 2024. The following Working Group members participated: Amy L. Beard, Chair (IN); Erica Weyhenmeyer, Vice Chair (IL); Richard Fiore (AL); Lori K. Wing-Heier and Chelsy Maller (AK); Gio Espinosa and Catherine O'Neil (AZ); Damon Diederich and Jennifer Bender (CA); Doug Ommen and Johanna Nagel (IA); Robert Wake (ME): Van Dorsey (MD); Jeff Hayden (MI); T.J. Patton (MN); Cynthia Amann (MO); Martin Swanson (NE); Santana Edison (ND); Michael Humphreys and Gary Jones (PA); Patrick Smock (RI); Frank Marnell (SD); Katie Johnson (VA); Todd Dixon (WA); Lauren Van Buren, Timothy Cornelius, and Andrea Davenport (WI); and Bryan Stevens (WY). Also participating was Kevin Gaffney (VT).

1. Adopted its July 10 Minutes

Commissioner Beard said the Working Group met July 10. During this meeting, the Working Group took the following action: 1) adopted its June 12 minutes and 2) discussed an approach for revising the *Privacy of Consumer Financial and Health Information Regulation* (#672).

The Working Group also met Aug. 5, in regulator-to-regulator session, pursuant to paragraph 8 (consideration of strategic planning issues) of the NAIC Policy Statement on Open Meetings, to discuss the Working Group's next steps.

Edison made a motion, seconded by Amann, to adopt the Working Group's July 10 (Attachment Six-A) minutes. The motion passed unanimously.

Beard provided a brief recap of the work done since the Spring National Meeting when the Working Group reformed. She said the Working Group held an open meeting in May, where a privacy expert from Husch Blackwell presented on federal and state privacy legislation, and the Working Group received the industry's draft, which uses Model #672 as a framework. She said public comments were requested and received on whether to continue work on the new Model #674 or to revise an existing NAIC privacy model while taking into consideration the option of utilizing the revised Model #672 provided by the industry.

During the Working Group's June 12 open call, Commissioner Beard said the Working Group heard from members, interested regulators, and interested parties; discussed their comments; and voted to move forward with revising Model #672. On July 9, Beard said Working Group leadership met with 20 NAIC Consumer Representatives to hear comments specific to consumer needs. She said the call was productive and provided insight into the issues that are most important to consumers. Beard said that during the July 10 open call, the importance of transparency throughout the process was emphasized, and leadership noted that regardless of the framework used, the discussion around core privacy principles and protections would be open and collaborative.

2. Heard an Update on Federal Privacy Legislation

Shana Oppenheim (NAIC) said the American Privacy Rights Act of 2024 (APRA) would establish national consumer data privacy rights and set standards for data security. The bill also would require covered entities to be transparent about how they use consumer data and give consumers the right to access, correct, delete, and export their data, as well as opt out of targeted advertising and data transfers. The measure would set standards for data minimization that would allow companies to collect and use data only for necessary and limited purposes and prohibit the transfer of sensitive covered data to third parties without the consumer's affirmative express consent. The Federal Trade Commission (FTC), state attorneys general, and consumers could enforce violations of APRA.

Oppenheim said the House Committee on Energy and Commerce released APRA in April 2024 by Chair Rep. Cathy McMorris Rodgers (R-WA) and Senate Commerce Committee Chair Sen. Maria Cantwell (D-WA). She said an updated version of the bill was released 36 hours before the markup in late June and was abruptly canceled five minutes before the meeting after heavy pushback from top GOP leadership, tech lobbyists, and privacy advocates. She said no markup had been rescheduled so it was too early to know the timeline before the August recess and fall elections.

Oppenheim said some of the groups against it include: 1) law enforcement groups, which say giving individuals the right to request the deletion of their data from brokers could rob law enforcement of access to "common investigative research services and other investigative tools that are used successfully every day by local, state, and federal law enforcement agencies;" 2) the Interactive Advertising Bureau (IAB), representing 700 media companies, which said a) opt-in for sensitive covered data (ordinary browsing history) would be bad for targeted advertising, b) the exemption for small businesses was not practical because most of them use third-party online advertising to grow, c) preemption was not complete enough, and d) a private right of action would be bad; 3) United for Privacy, which said more preemption is necessary to create a uniform national privacy standard; 4) the Main Street Privacy Coalition (made up of 20 national trade associations), which is concerned with customer loyalty programs, common branding, and private right of action that would equate to a trial lawyer bonanza.

Oppenheim said APRA would apply to companies subject to the FTC Act, and even goes a step farther to reach nonprofit entities (covered entities). She said some small businesses (under $40 million in revenue and processing covered data of less than 200,000 individuals) would be exempt unless they generate revenue from sharing covered data with third parties. The APRA would cover all individuals and treat information about minors (defined as individuals under the age of 17) as sensitive covered data.

She also said covered data includes information that identifies or is linked or linkable to an individual or a device that is linked or linkable to one or more individuals. Oppenheim said this broad definition does not include de-identified data, employee information, publicly available information, inferences made exclusively from multiple independent sources of publicly available information (with certain conditions), or information in collecting a library, archive, or museum. She said sensitive covered data includes the same categories in state privacy laws, such as information revealing race, ethnicity, national origin, sex, government-issued identifiers (e.g., a social security number or driver's license number), information that describes an individual's past, present, and future health conditions and treatments, genetic information, financial account information, biometric information, or precise geolocation information. Oppenheim said the APRA considers private communications, account or device log-in credentials, information revealing sexual behavior, information regarding minors, images and recordings intended for private use or depicting the naked or undergarment-clad private area of an individual, an individual's viewing log video programming, information revealing an individual's online activities across websites, and other information the FTC determines to be sensitive covered data.

Oppenheim said the APRA requires covered entities to provide consumers with rights about their covered data and how it may be processed. She said these rights include the right to access their covered data, the correction of their covered data, the deletion of their covered data, and the right to the portability of their covered data. Oppenheim said covered entities must have flexibility and agility in their data storage practices, allowing for deletion or correction and providing portability. For example, if an individual requests a copy of all their covered data collected, the covered data can be exported in an accessible manner to be shared with the individual. These rights apply even if that data is going to be shared with a competitor or made public (except for derived data if it would result in the release of trade secrets or other proprietary or confidential data). Oppenheim said the APRA allows consumers to opt out of covered data processing and covered data use, including opting out of targeted advertising, algorithmic decision-making, and covered data transfers. She said the opt-out process should be straightforward and transparent. Oppenheim said the APRA further directs the FTC to establish requirements and technical specifications for a centralized mechanism for opt-outs within two years of the APRA's enactment.

She said the previous version included that for covered entities using algorithmic decision-making, and the APRA requires a clear and conspicuous notice to individuals that provides meaningful information on how the algorithm makes or facilitates a consequential decision—i.e., decisions that affect an individual's housing, employment, education enrollment, health care, insurance, or credit opportunities. Oppenheim said the APRA emphasizes that covered data should be restricted to specific, expected uses. She said this mirrors the language used in the General Data Protection Regulation (GDPR) of the European Union (EU) regarding data minimization and requiring a clear purpose for data collection. Oppenheim said covered entities and their service providers should closely examine their data collection practices and avoid the "collect-everything-we-can-and-sort-it-out-later" mentality. All information collected and retained should have a clear, explicit, and specified purpose.

Oppenheim said covered entities with more than $250 million in revenue and that collect large amounts of covered data or sensitive covered data (large data holders) must conduct privacy impact assessments (PIAs), which evaluate the impact of proposed data processing on privacy, to consider the potential risks and benefits of data collection. She said the previous version said covered algorithms were a computational process that makes a decision or facilitates human decision-making by using covered data, are also subject to impact assessments, and large data holders are required to detail the steps taken to mitigate the risk of harm to the following: minors, housing, education, employment, health care, insurance, credit opportunities, public accommodations based on protected characteristics, or disparate impacts based on such characteristics or on political party affiliation. Additionally, it said these PIAs and covered algorithm impact assessments should be transparent and clearly articulated, with recommendations to manage, minimize, or eliminate privacy-related impacts on a community.

Oppenheim said covered entities and service providers are required to have one qualified employee to serve as a privacy or data security officer. She said large data holders would be required to have two officers—a privacy and a data security officer. The data security officer must be a designated, qualified employee who oversees the organization's data protection efforts and ensures compliance with the APRA's requirements regarding consumer privacy rights, data minimization, and cybersecurity measures. Oppenheim said large data holders that trigger this requirement would be required to annually certify to the FTC their internal controls for APRA compliance and the reporting structure for the data security officer and other certifying officers, including the company's CEO.

Oppenheim said the APRA would permit individuals to sue with a private right of action for violations of the APRA. She said the legislation would not allow for mandatory arbitration clauses if the case involves minors, substantial privacy harm ($10,000), or specific physical or mental harm. She also said an individual may seek actual damages, injunctive relief, declaratory relief, reasonable attorneys' fees, and litigation costs. Oppenheim said this provision could lead to class action lawsuits and is very controversial. She said in addition to individuals, the FTC or state attorney generals may also enforce the APRA. Oppenheim said non-sectoral state privacy laws are preempted by the APRA, which means laws that address specific subsections of privacy rights, including employment, education, breach notifications, banking, health, and other narrow laws, are not preempted, but privacy laws that generally address all categories of personal data and all rights to the data as provided in the APRA will be superseded by the APRA. She said this can help to simplify the U.S. data privacy framework, but not all state regulators are happy with this idea based on the APRA having broader or narrower protections in comparison to their own laws.

Oppenheim said new sections in APRA 2.0 include a new section on the Children's Online Privacy Protection Act (COPPA 2.0) under Title II, which differs to a certain degree from the COPPA 2.0 proposal currently before the Senate (e.g., removal of the revised "actual knowledge" standard and removal of applicability to teens over age 12 and under age 17). She said the revised APRA draft includes a new dedicated section on privacy by design that requires covered entities, service providers, and third parties to establish, implement, and maintain reasonable policies, practices, and procedures that identify, assess, and mitigate privacy risks related to their products and services during the design, development, and implementation stages, including risks to covered minors.

Oppenheim said as an exception to the general data minimization obligation, the revised APRA draft adds another permissible purpose for processing data for public or peer-reviewed scientific, historical, or statistical research projects. She said these research projects must be in the public interest and comply with all relevant laws and regulations. If the research involves transferring sensitive covered data, she said the revised APRA draft requires the affirmative express consent of the affected individuals. Oppenheim said the revised APRA draft expands obligations for data brokers by requiring them to include a mechanism for individuals to submit a "delete my data" request. She said this mechanism is like the California Delete Act in that it requires data brokers to delete all covered data related to an individual that they did not collect directly from that individual if the individual so requests. While the initial APRA draft required large data holders to conduct and report a covered algorithmic impact assessment to the FTC, if they used a covered algorithm posing a consequential risk of harm to individuals, the revised APRA requires such impact assessments for covered algorithms to make a "consequential decision." She said the revised draft also allows large data holders to use certified independent auditors to conduct the impact assessments, directs the reporting mechanism to the National Institute of Standards and Technology (NIST) instead of the FTC, and expands requirements related to algorithm design evaluations. Oppenheim said while the initial APRA draft allowed individuals to invoke an opt-out right against covered entities' use of a covered algorithm to make or facilitate a consequential decision, the revised draft now also allows individuals to request that consequential decisions be made by a human. Oppenheim said the revised APRA draft's definition section includes new terms, such as "contextual advertising" and "first-party advertising." She said the revised APRA draft also redefines certain terms, including "covered algorithm," "sensitive covered data," "small business," and "targeted advertising."

Because the act is intended to establish a uniform national data privacy and data security standard, Oppenheim said it would preempt state law. However, she said the act also enumerates extensive exceptions that would preserve provisions of state laws related to employee privacy, student privacy, data breach notifications, and health privacy. Oppenheim said the APRA would also preserve several rights to statutory damages under state law. For example, in civil actions brought for violations related to biometric and genetic information in Illinois, the act would preserve relief set forth in the Illinois Biometric Information Privacy Act (BIPA) and Genetic Information Privacy Act (GIPA). Oppenheim said the act would also preserve statutory damages for security breaches under the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA). She said these rights would be preserved as the statutes read on Jan. 1, 2024. Like the American Data Privacy and Protection Act (ADPPA), she also said APRA would preempt comprehensive state data privacy laws, except for an enumerated list of current state laws, including consumer protection laws of general applicability and laws addressing employee privacy, student privacy, and data breach notification. Oppenheim said APRA would also broadly exempt "any data subject to" and in compliance with the requirements of Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) (GLBA); however, APRA does not specify whether state GLBA laws would likewise be preempted. As a result, for some entities, she said APRA may create a new layer of compliance requirements, requiring those entities already subject to state-implemented GLBA privacy regimes to also be subject to oversight by the FTC.

3. Heard a Presentation from Consumers' Checkbook on Legacy Systems and the Protection of Consumers' Privacy

Eric Ellsworth (Consumers' Checkbook) said he is the director of health data strategy and that he has 25 years of experience in data science and software/IT management. As such, he developed, deployed, and decommissioned IT systems under privacy regulations. As the Health Insurance Portability and Accountability Act of 1996 (HIPAA) chief security officer in a clinical laboratory, he created and oversaw the organization's HIPAA program. Ellsworth said he advocates for transparency and simplification of the consumer experience. He said insurers are at considerable risk of data breaches because they are high-value targets with lots of data and money. According to the 2022 Black Kite Cyber Insurance Report, more than 50% of the largest insurance carriers are three times more likely to experience breaches than the best-protected organizations. Ellsworth said potential losses and disruptions include an average ransomware cost of $4.65 million; regulatory fines; customer lawsuits; operational paralysis of 22 days for ransomware, which typically takes longer to fix and restore systems; premium increases to pay for company costs; and damage to the company's brand. He said insurer insolvency can damage entire markets as one company's practices can affect customers of many other companies.

Ellsworth said data privacy and cybersecurity are different but linked. He said cybersecurity means protecting information assets from intrusion. It is like having a fence, guards, and alarms around a warehouse. These items do not control what goods are stored or where they are shipped. He said data privacy is putting controls on how data is stored, used, and transmitted. He said deletion requests mean "to destroy all items from supplier A," while opt-out means "don't send supplier B's gray pants to Canada." Ellsworth said a company can have sufficient cybersecurity measures but no control over data flows, but that protecting consumers' privacy requires both. He said consumer privacy rights require controlling data flows, which answers where a consumer's data is stored, where it is being sent, and when a consumer exercises these rights, how the company will find their data and fulfill the request. This leads to legacy systems and legacy data. He said legacy systems are software that is outdated but still operational. It is no longer actively being maintained, upgraded, or supported, and there is no personnel with active knowledge of how the system works or what is in it. Many are still used for core business functions and often serve as only a way to access old records.

Ellsworth said legacy data is data that is stored in old systems via email, spreadsheets, hard drives, old servers, or with third-party providers. He said it is a default state of affairs where nobody has a full picture of what or where the data is. He said legacy systems are highly vulnerable and pose ever-increasing challenges to meeting privacy and security requirements. Ellsworth said delays in fixing or replacing legacy systems would increase costs, be more time-consuming, provide less support, be harder to find talent, and make purchasing cyber insurance difficult or more expensive. He said regulators and insurers should be accounting for costs and risks around legacy systems regardless of whether insurers can replace them now.

Ellsworth said insurers may not be able to get rid of all legacy systems, but they need to put into place organizational controls typically required to obtain cyber insurance to ensure that they collect, store, and use data in ways that protect privacy and ensure the ability to delete, modify, and account for data upon request. He said examples of control processes are maintaining inventory of which systems contain which data; training on how data can and cannot be used; approving IT systems and storage for sensitive consumer data (e.g., "secure folders"); and requiring approvals for new uses or transmissions of data. He said legacy systems can be assessed for risks, costs to keep and replace, and effects on consumers' rights to delete or opt out of data sharing within these organizational controls. Ellsworth said HIPAA is America's earliest and most broadly implemented privacy law with many of its conceptual parallels to the current model and in the CCPA. He said adopting HIPAA took work but was doable. Ellsworth said covered entities became accountable for safeguarding private information both in their own organizations and when sharing with third parties (business associates) and underwent organizational process and culture changes to bring control to their collection, use, and sharing of data. He also said health insurers were not bankrupted. Now, health insurers are rightfully concerned about uncontrolled disclosures and are upset by federal rules permitting app developers to access data without a business associate agreement.

Ellsworth said his recommendations for organizational controls are that: 1) the model law explicitly requires insurers to institute organizational controls around the collection, storage, and use of data with executive or board-level accountability mechanisms; 2) regulatory oversight of these processes use a risk-based model to allow insurers latitude while ensuring protection of consumers' privacy with legacy system risks being addressed within these assessments, and financial risks arising from legacy system vulnerabilities be considered; and 3) regulators leverage other work in assessing quality of insurers' privacy and security controls, such as cyber insurance assessments, HIPAA, and/or CCPA controls and documentation.

He said his recommendations for third-party service providers are that: 1) the model law imposes requirements on insurers in diligence and contracting with third parties; 2) obligates insurers to assess the capability of the third party to comply with contractual terms required under this model law; and 3) requires insurers to control and audit their accounts and set up with third-party service providers.

Ellsworth said his recommendations for timelines for deletions and modifications are that: 1) when a consumer requests deletion or modification of data, that data be deleted or de-identified within 45 days of receipt of request, and if additional time is needed, allow 45 more days to delete, provided the licensee explains to their state regulator why additional time is needed and the consumer is notified; and 2) state privacy laws setting these timelines mimic those in California, Colorado, Connecticut, Utah, or Virginia. He said additional recommendations are that: 1) if licensees demonstrate that full deletion is not possible, licensees should make best efforts to restrict access to and use of the data on legacy systems by masking or encrypting data so it is not readable; putting strict access controls in place so data is not accessible for use; and creating a "restriction list" to flag data that should not be used, even if is not deleted; and 2) apply administrative sanctions or financial penalties, where licensees do not show good faith efforts to comply.

4. Discussed its Next Steps

Commissioner Beard reminded the Working Group that its charges for 2024 are to update Model #672 in a transparent manner that is feasible and adaptable so states can implement it. She said a chair draft revising Model #672 was distributed to Working Group members and interested regulators for their review in advance of the Summer National Meeting. She said the chair draft is intended to serve as a starting place for the drafting group to begin their work, and it is not designed to represent any agreement or position of the Working Group. Beard said the chair draft includes pertinent information and principles pulled from the *NAIC Insurance Information and Privacy Protection Model Act* (#670), draft Model #672 Plus, draft Model #674, and state comprehensive privacy laws. She also said the chair draft focuses on four key privacy principles and believes the language and principles will be familiar to everyone from previous drafts and conversations: third-party arrangements; right to access, correct and delete; sale of personal information; and handling of sensitive personal information. Once again, Beard said she wanted to stress that the chair draft is meant to be a starting point for discussion, and none of the language has been finalized, so comments and discussion are welcomed and encouraged, as the group looks forward to seeing how the draft evolves to create consensus among Working Group members, interested regulators, and interested parties.

Commissioner Beard said the chair draft would be exposed to the public for a 30-day comment period following the Summer National Meeting. She said Lois Alexander (NAIC) would include an invitation for drafting group volunteers and guidelines for drafting group participation in the exposure draft email. Commissioner Beard said Weyhenmeyer would lead the drafting group, which will be open to regulators and interested parties. She said the guidelines for drafting group participation are intended to set expectations for drafting group members and promote productive drafting conversations. She said the Working Group will continue to hold open and regulator-only sessions, as needed, to determine the best privacy regime and draft a model law that reflects that. She said the Working Group also wanted to ensure that everyone understands the next steps in this process and their respective roles and responsibilities. Beard said the Working Group wants to hear from all parties and encouraged their participation by submitting comments and redlines during public comment periods and engaging with the drafting group.

Weyhenmeyer said comments will be requested on third-party arrangements only during the first 30-day exposure period.

Harry Ting (Healthcare Consumer Advocate) said he submitted comments prior to the Summer National Meeting and asked if they could be distributed now. Commissioner Beard said the comments would be considered with the other comments received during the exposure period. Silvia Yee (Disability Rights, Education, & Defense Fund) said regulators are the heroes in the consumer data privacy arena, as they have the power and authority to help humanity or not. She also said she would be happy to help the Working Group in any way she can.

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

SharePoint/NAIC Support Staff Hub/Committees/H Cmte/ 2024 Summer/Privacy/Minutes/Minutes-PrivacyWG081424.docx