Draft: 1/4/23

Privacy Protections (H) Working Group
Tampa, Florida
December 12, 2022

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Tampa, FL, Dec. 12, 2022. The following Working Group members participated: Katie Johnson, Chair, represented by Don Beatty (VA); Cynthia Amann, Co-Vice Chair (MO); Chris Aufenthie, Co-Vice Chair (ND); Chelsy Maller (AK); Shane Foster (AZ); Damon Diederich (CA); George Bradner and Kristin Fabian (CT); Erica Weyhenmeyer and C.J. Metcalf (IL); LeAnn Crow (KS); Ron Kreiter (KY); Van Dorsey (MD); Robert Wake and Benjamin Yardley (ME); Martin Swanson (NE); Teresa Green (OK); Raven Collins represented by Numi Griffith (OR); Gary Jones (PA); Frank Marnell (SD); Todd Dixon (WA); and Lauren Van Buren, Rachel Cissne Carabell, and Timothy Cornelius (WI). Also participating were Sarah Bailey (AK); Glenda Haverkamp (KS); Kathleen A. Birrane (MD); John Arnold (ND); and Tanji J. Northrup (UT).

1. Adopted its Summer National Meeting Minutes and Noted an Updated Work Plan

Amann said the Working Group met Aug. 9.

Commissioner Birrane made a motion, seconded by Diederich, to adopt the Working Group's Aug. 9 minutes (*see NAIC Proceedings – Summer 2022, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Four*). The motion passed unanimously.

Amann noted that an updated Nov. 11, 2022, work plan for the Working Group was posted to the Working Group's web page.

2. Heard Updates on State Privacy Legislation

Jennifer Neuerburg (NAIC) said there was little action on state privacy legislation, and both updated charts were posted to the Working Group's web page.

3. Heard a Presentation from a Consumer Perspective on General Market Practices Regarding the Use of Personal Information During the Insurance Process

Matthew J. Smith, Esq. (Coalition Against Insurance Fraud—CAIF) said the data onslaught is here, and insurance consumers need state insurance regulators to make sure they are protected. He said data, if used correctly, can be used in helping consumers with lower premiums; tailoring coverages; and making the insurance process of application, payment, and claims easier. However, he said regulatory oversight and accountability are crucial. He said there is support for the appropriate use of data in the world of insurance, and consumers are not data-ignorant according to "The Ethical Use of Data to Fight Insurance Fraud Study" commissioned by the CAIF and executed by Dynata with a recommendation from NAIC consumer representative, Brenda J. Cude (University of Georgia). He said this study was done to help guide state insurance legislators and regulators because it includes valuable insight to guide the proper oversight of data both in antifraud and beyond. He said the study had over 2,000 American respondents, with 67% of those responding being consumers; 17% insurance professionals; 6% federal and state legislators, regulators, or government agency respondents; and 10% from the legal or data service industry. He said the data collected was cross-analyzed and confirmed by data scientists as having no

 

difference from consumers to companies to other respondents. The study showed that 85% of all American consumers are concerned about data fraud in insurance transactions. Smith said when consumers were asked about whom they trust with their personal data, 75% said they were okay with insurance companies using their data, but 61% wanted a national data protection standard enforced by state insurance departments, and 85% supported data laws and guidance for insurance companies' use of such data. He said disclosure regarding data usage and clarity—i.e., requiring companies to have a straightforward and easy-to-read privacy policy—are key to insurer data trust. He said when the premium is reduced to receive data, 61% of respondents said they had no expectations; however, 46% said they expected a 10% reduction in premium. He said when asked if insurers are properly overseeing personal data, insurance professionals said 47% of their companies had strong data protections in place, and 53% said their companies had little, not good, or no policy of personal data protection in place.

Smith recommended that state insurance regulators play a strong role by using the results of this study in consultation with data scientists to: 1) apply this data to their work both nationally and at the state level; 2) encourage others to undertake similar research; 3) address data usage at all parts of the insurance transaction; 4) create clear policies with accountability; 5) share information with other states; 6) control the use of personal data for marketing; 7) create standards for data use and retention after cancellation or non-renewal; 8) determine if data is being de-identified and, if so, by whom; 9 ) include third parties who aggregate or oversee programs for insurers; 10) track the shipping of data overseas; 11) address bias and prejudice; and 12) determine whether the misuse of personal data is intentional or unintended. In closing, he said the challenge moving forward is getting it right and right away, as there is no time to continue to simply wait and see what happens with the use of insurance consumers' personal data.

4. Heard a Presentation from a Company Perspective on General Market Practices Regarding the Use of Personal Information During the Insurance Process

Scott Fischer (Lemonade Insurance Company) said we all use data in our daily lives; however, a balance is needed for the necessary use of data and the consumers' need for privacy. He said insurance is unique with open questions that still need to be addressed. He said one question has to do with the best way to handle tradeoffs, because we need to ensure that users cannot manipulate data for fraud detection and how much transparency companies can provide. He said another question is regarding what level of control users can have, because users who choose to delete their data give up a less personalized experience. For auto insurance, he said allowing for consumer deletion of data would skew the company's perception of risk.

Fischer said the question includes determining the best way to provide users with the appropriate context; whether it should be through disclosures, terms of service, or privacy policies; as well as what such notices could or should look like. He said this unique insurance industry should think about privacy by its intentional collection and use of a user's data.

Fischer said companies should look at: 1) what type of data is being collected from users and why it is being collected; 2) who has access to that data and what they can use it for; 3) what users know about their data and what control they have; and 4) how it is collected.

Fischer said data that is sensitive and personal should come directly from the user; data that relates to user behavior in other domains, such as a house purchase, comes from third-party sources; user behavior data, like scrolling through the product online, is provided indirectly; and data about a user that is generated via machine learning (ML), such as whether the user has a swimming pool, is generated within the company itself.

Fischer said user data ranges in its sensitivity from less sensitive data that is not user-identifiable, such as scrolling patterns, to more sensitive data that is considered sensitive personally identified information (SPII), such as one's Social Security Number (SSN) or biometrics that could cause significant harm if compromised, with the midpoint data being user identifiable and personal, such as video footage. He said the sensitivity of the data should be used to control how each category of data is collected, what user controls should exist, and who can access the data internally and externally. He said the more sensitive the data is, the more guarded access to the data should be and the more control and awareness users should have. He said less sensitive data can be indirectly collected and stored without explicit consent and provided more broad access and use across use cases and features. He said access to more sensitive data should be extremely limited internally and used only for a handful of purposes where no other data can be used and explicit user permission to collect or generate data must be sought, and it should allow users controls to be able to access and delete data. At the midpoint, he said limited access is allowed for purposes that are pre-defined for users, and it provides users with appropriate levels of awareness and control depending on the use case.

Fischer said state insurance regulators need to hold third-party sources accountable for clarity during collection; the purpose should be clear to users throughout the user experience for data obtained directly from users; indirect behavioral data should not contain any sensitive information, such as personally identified information (PII); and when users provide information for generation within the company, users should be informed of how data may be used, especially for more sensitive cases.

Fischer said companies should provide users with the proper context while the data is being collected; provide a common help center or space for users to understand what data is being collected, and for what purposes; clearly indicate to users that account deletion equals data deletion; and identify what data makes sense for a user to have control over in terms of deletion, access, and usage. He said there are technical innovations like differential privacy and federated learning in this space that are making it possible to add noise to or silo a user's data, while still providing access to train models. However, he said these innovations are not being used in the insurance space yet. It would provide a secure environment where personal data could be stored and subjected to a differentially private computation with access to analysts' queries via noisy results.

5. Discussed General Market Practices Regarding the Use of Personal Information During the Insurance Process from Both Perspectives

Eric Ellsworth (Consumers' Checkbook) said as a data scientist, he believes data becomes much more sensitive, as data is linked to other data; it is necessary to flag the linkage aspect and relevancy coalescent, as well as tangential relationships. Harry Ting (Health Consumer Advocate) said Smith's survey clearly indicates that state insurance regulators can and should regulate insurance companies' use of consumer data even though the Metas like Google are too big to fail and control. Wake said there is a strong push from the federal government to put together a list of things states can and cannot regulate. He said identity theft protection is not all there is to protect; there is also the universe of third parties to consider. He said federal Health Insurance Portability and Accountability Act of 1996 (HIPAA)-like concessions are needed, with third parties agreeing to keep all data protected like it is under HIPAA. He said state insurance regulators need to think about the purposes for which data is to be used and the companies who do things behind the scenes to support insurance companies. He said there is a dichotomy between universally available data and non-public data. He said telematics are needed by auto insurance companies with things like coverage, uber, etc. included. Smith said according to the CAIF's study, car trackers are not all altruistic.

Amann said the new *Insurance Consumer Privacy Protection Model Law* (#674) draft includes all lines of business. She said the drafting group discussed federal acts and focused on being technologically current. Commissioner Birrane said she has confidence in state insurance regulators to develop a model that all states can use to effectively regulate and serve consumers.

6. Discussed Other Matters

Amann reminded attendees about the upcoming exposure draft of Model #674 at the end of January for a two-month comment period to be followed by open meetings resuming in March to discuss all comments received in the coming months.

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

SharePoint/NAIC Support Staff Hub/Member/H Cmte/Privacy/Minutes_2022 Fall National Meeting_PPWG

 