CLIENT ALERT

NAIC Proposes New Consumer Privacy Model Law for the Insurance Industry

February 13, 2023

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Kara Baysinger | Stephanie Duchene
Allison J. Tam | Michelle Bae

On February 1, 2023, the National Association of Insurance Commissioners ("NAIC") Privacy Protections Working Group (the "Working Group") released an exposure draft of a new Consumer Privacy Protections Model Law ("Model 674").[1] The current privacy-related NAIC model laws are decades old — the Insurance Information and Privacy Protection Model Act ("Model 670") is almost 40 years old and has been enacted by 17 states, and the Privacy of Consumer Financial and Health Information Regulation ("Model 672") was adopted in the wake of the enactment of the Gramm-Leach-Bliley Act ("GLBA") over 20 years ago and has been enacted in 43 states. The goal of Model 674 is to replace these two model laws with an improved and modernized model law that incorporates key concepts in existing privacy and data protection laws — including aspects of recently enacted privacy laws such as the California Consumer Privacy Act ("CCPA").[2] The published Model 674 exposure draft attempts to accomplish this by adopting an expansive scope (e.g., applying to both licensees and, for the first time, service providers) and incorporating a number of concepts (including restrictions on cross-border transfers of personal information) that are likely to have broad implications for companies in the insurance industry.

Model 674 is still in draft form, and interested stakeholders have an opportunity to push for changes. The Working Group has explained that it plans to conduct outreach throughout February with affected companies, and that additional

1 *Exposure Draft of the New Consumer Privacy Protections Model Law #674*, NAIC (Feb. 1, 2023), available at https://content.naic.org/sites/default/files/inline-files/Exposure%20Draft-Consumer%20Privacy%20Protection%20Model%20Law%20%23674%201-31-23.pdf.

2 *Request for NAIC Model Law Development*, NAIC (July 27, 2022), available at https://content.naic.org/sites/default/files/inline-files/Attmt%203_MLR_670and672-Request.pdf.

discussion on Model 674 will take place during the NAIC's Spring National Meeting, currently scheduled for March 22–25, 2023. In addition, the exposure draft for Model 674 is subject to a sixty (60)-day comment period — interested companies have until April 3, 2023 to submit comments, suggestions, and proposed revisions. According to the Working Group's publicly available work plan,[3] it is expecting to vote on the revised draft at the NAIC's Summer National Meeting, which is scheduled for August 13–17, 2023. Once finalized, Model 674 would need to be enacted on a state-by-state basis before it comes into effect in each jurisdiction.

Model Law 674: More Modern…and More Burdensome?

Given recent trends in data protection and privacy laws, highlighted by the General Data Protection Regulation ("GDPR") in the European Union and the CCPA and other recently enacted state laws in the United States ("U.S."), it is not surprising that Model 674 adopts a more restrictive approach to the collection and use of personal information. However, there are a number of provisions in the exposure draft that would likely have significant—and potentially material—implications for companies in the insurance industry.

Scope — Covered Entities and Covered Data

Consistent with recent trends, Model 674's scope is much more expansive than either Model 670 or Model 672. Among other things, Model 674 would:

- Apply to both licensees *and* third-party service providers that engage in any covered activities[4] (neither Model 670 nor Model 672 applied directly to third-party service providers);
- Expand the definition of "personal information" beyond the definition in Models 670 and 672, and even beyond CCPA (in particular, CCPA excludes "publicly available" information from the definition of "personal information," but Model 674 does not); and
- Include as new categories of "personal information" newly defined terms "sensitive personal information" and "biometric information," which largely mirror the definitions under the CCPA.

[3] *Privacy Protections Working Group Work Plan*, NAIC (Feb. 1, 2023), available at https://content.naic.org/sites/default/files/inline-files/PPW%20Workplan%20Rev%203%20111022.xlsx.

[4] These include: (1) collecting, processing, retaining, or sharing consumers' personal information in connection with insurance transactions; (2) engaging in insurance transactions with consumers; or (3) engaging in additional permitted transactions involving consumers' personal information. "Additional permitted transactions" means collecting, processing, retaining, or sharing a consumer's personal information, with the consumer's consent, for either (a) marketing purposes or (b) research activities not related to rating or risk management purposes for or on behalf of the licensee.

Regulated Activities — New Obligations and Requirements

Model 674 would impose a number of requirements and obligations that would be new to the insurance industry. In particular, the proposed restriction on cross-border data transfers and the requirement to conduct extensive diligence of third-party service providers could have important operational implications for many companies, and the specter of a private right of action opens the door to significant liability for even immaterial or inadvertent violations.

New "Prior Consent" Requirement for Cross-Border Transfers of Personal Information. Under Model 674, a licensee or third-party service provider would be required to obtain "prior consent" from any consumer whose personal information will be shared with a person outside the U.S. or its territories.[5] Licensees also would be required (i) to allow consumers to revoke their consent for cross-border data transfer, and (ii) to delete any of a consumer's personal information stored overseas upon revocation of previously given consent. These obligations would be entirely new to U.S. privacy laws, but are becoming increasingly popular around the globe after the adoption of similar restrictions in GDPR. The stated policy reason for this provision is to protect consumers' *sensitive* information from being shared with countries outside the U.S. where there may not be any privacy laws protecting such information. However, as currently drafted, Model 674's requirement is both too broad (it would apply to *any* sharing of a consumer's personal information outside the U.S.) and too narrow (consumers could conceivably consent to sharing data with countries regardless of the strength of existing privacy laws in those jurisdictions). And as a practical matter, the GDPR experience affirms that such a requirement would introduce significant friction into even intracompany data processing activities, likely forcing companies with multinational operations to locate and source some—and maybe all—of their back office and other data processing activities in the United States.

New Requirements for Licensees and Third-Party Service Providers. Model 674 would require licensees to conduct extensive diligence and oversight on third-party service provider arrangements — a requirement that does not exist under Models 670 and 672, but does exist in current cybersecurity and data security model laws. In addition, licensees and third-party service providers would be required to enter into a written agreement that requires the third-party service provider to comply with both Model 674's requirements *and* the licensee's own practices with respect to the collection and use of consumers' personal information. The agreement also would need to specify that the third-party service provider may not further share or process a consumer's personal information for any purpose other than what is specified in the agreement. Many licensees already undertake similar efforts to comply with cybersecurity regulations (such as the New York State Department of Financial Services Cybersecurity Regulation), but they would need to significantly expand such efforts to comply with the requirements of Model 674.

New Private Right of Action. Primary enforcement authority under Model 674 would belong to the state insurance regulator, but the exposure draft of Model 674 includes an "optional" private right of action that would allow consumers to

[5] It is not clear what form that prior consent must take. In other provisions, Model 674 speaks specifically of "written consent," but in other provisions explains that any consent under the Model Law must be written.

pursue litigation in the event of a licensee's or its third-party service provider's failure to comply with Model 674. The private right of action as currently drafted would be subject to certain limitations to try to make it more palatable—e.g., it cannot be brought unless there is an actual victim and damage, it would be limited to actual damages, it is subject to a two-year statute of limitations, and class actions would not be permitted—but opening the door to such actions relates substantial risk that a state may adopt a broad private right of action.

Other new requirements that would be imposed under Model 674 are less groundbreaking, but still could have important operational and practice implications. For example:

- **Data Minimization.** Model 674 would introduce a new data minimization requirement, under which a licensee's collection, processing, retention, and sharing of consumers' personal information would need to be reasonably necessary and proportionate to achieve the purposes related to the requested insurance transaction or additional permitted transactions, and not further processed, retained, or shared in a manner that is incompatible with those purposes. Strict enforcement of such a requirement, without further guidance, could create significant risk and uncertainty.

- **Data Retention.** Model 674 would impose new data retention and deletion requirements by expressly identifying permitted purposes for retaining consumers' personal information, and requiring the licensee to completely delete all of a consumer's personal information within ninety (90) days once the permitted purpose no longer applies. Third-party service providers would be required to certify to the licensee that all of the consumers' personal information has been deleted. Furthermore, if the licensee no longer has a relationship with a consumer in connection with any insurance transaction, the licensee would be required to send a notice to the consumer informing such consumer that the licensee and any third-party service provider no longer retain any of the consumer's personal information. Licensees would be required to develop policies and procedures to comply with the retention and deletion requirements.

- **Privacy Notice.** Model 674 would not change the requirements for an initial and an annual privacy notice, but licensees would be required to include much more information in such notices than under Model 670 or 672. For example, the privacy notices would need to include (i) descriptions of the licensee's requirement to obtain consent for certain purposes and how a consumer may provide and revoke consent; (ii) a summary of the reasons for the licensee's collection and use of personal information and the approximate period of retention; and (iii) a statement that no licensee or third-party service provider may sell or share for valuable consideration a consumer's personal information. Additionally, a licensee would need to include in its privacy notice a statement describing its collection, processing, retention, or sharing of personal information outside the U.S.

CCPA and Model 674

The issues presented by Model 674 are further complicated by the regulatory overhang of the CCPA. Of the five states that have passed comprehensive privacy laws, California alone does not provide an entity-level exemption for financial institutions subject to the GLBA. Instead, the CCPA only exempts the data subject to the GLBA and the California Financial Information Privacy Act; as a result, most insurers are likely subject to both the CCPA and the privacy and consumer protection provisions of the insurance laws in California.

The California Privacy Rights Act, which amended the CCPA and came into effect on January 1, 2023, includes language directing the newly established California Privacy Protection Agency (the "Agency") to address the potential consumer and industry confusion created by this dual set of statutory requirements. Specifically, the Agency is directed to review insurance laws that relate to consumer privacy and adopt regulations for the insurance industry to the extent existing insurance laws do not provide greater protection to consumers, but it has yet to address the issue and has not provided any concrete indication as to when it will. Although Model 674 appears to have considered and incorporated certain concepts and definitions from the CCPA, Model 674 and the CCPA do not perfectly align — for example, Model 674 does not incorporate a right to deletion because the Working Group determined that the needs of insurance companies made such a right unworkable, and instead decided to adopt strict data retention and deletion requirements. Whether the Agency would accept that different requirements may be appropriate—and sufficient—in different contexts is an open question.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Kara Baysinger
415 858 7425
kbaysinger@willkie.com

Stephanie Duchene
310 855 3066
sduchene@willkie.com

Allison J. Tam
212 728 8282
atam@willkie.com

Michelle Bae
202 303 1166
ebae@willkie.com