NAMIC
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

317.875.5250 | [F] 317.879.8408
3601 Vincennes Road, Indianapolis, Indiana 46268

202.628.1558 | [F] 202.628.1601
20 F Street N.W., Suite 510 | Washington, D.C. 20001

UNIFORM LAW COMMISSION

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT
DRAFTING COMMITTEE

April 9, 2020

On behalf of National Association of Mutual Insurance Companies (NAMIC)[1] members, thank you for the opportunity to share thoughts as the Collection and Use of Personally Identifiable Data Act (CUPIDA) drafting committee considers model approaches and wording. NAMIC understands that concepts and changes were discussed when the committee met in February. Because another version may already be in the process of being developed, these comments touch on just a few specific sections and they focus more broadly on important concepts. Also, given that some of the concepts and the wording appear to still be in the early stages, NAMIC reserves the right to modify items reflected in these comments as the process moves forward.

The objective of protecting consumers who wish to restrict information-related activity can be met under both an opt-in and an opt-out. No greater privacy protection is afforded under either approach to an individual wanting more restrictive data handing. Under both approaches the individual consumer controls the decision. The difference is the default automatic standard. An opt-in privacy mechanism may have a facial appeal initially, given its apparent simplicity. However, it seems this approach may offer fewer choices to consumers because it assumes that consumers value restrictions over the benefits of product and service variety, innovation, and/or ease of use. Not only may an opt-in be more costly to administer because it would require companies to obtain consent, but customers may perceive it as more intrusive due to increasing contacts with the customer in an effort to secure consent. As discussed in this statement, especially in the context of insurance, an opt-in could have meaningful consequences.

INSURANCE INDUSTRY – LAWS/REGULATIONS & BUSINESS PURPOSE

As the Committee acknowledges in Section 3 addressing SCOPE, some entities are already highly regulated with respect to personal information. Two areas already contemplated in the draft are personal health information under the Health Information Portability and Accountability Act (HIPAA) and consumer reporting agency information under the Fair Credit Reporting Act (FCRA).

[1] NAMIC is the largest property/casualty trade association in the US, serving regional and local mutual insurance companies on main streets across America as well as many large national insurers. NAMIC membership includes more than 1,400 insurance companies. NAMIC member companies write $268 billion in annual premiums. Our members account for 59% of homeowners, 46% of automobile, and 29% of business insurance markets.

Financial services also would be appropriate to exclude from the scope. This could be accomplished with wording like:

> This act does not apply to a financial institution or any of its affiliated companies that are subject to Title V of the federal "Gramm-Leach-Bliley Act of 1999," 15 U.S.C. s.6801 et seq. and the rules and implementing regulations promulgated thereunder or to [INSERT RELEVANT STATE PRIVACY LAW] et seq. and the rules and implementing regulations promulgated thereunder.

For your background, let us share more information about some of the relevant legal and regulatory landscape. New provisions would not be enacted in a vacuum. This is especially true for the insurance industry. The insurance industry's consumer protections, through robust laws and regulation, have been in place for over one hundred and fifty years. Each state and the federal government already have laws/regulations to address data privacy, security, and other requirements. By recognizing that this is not a blank slate and to help avoid confusion and conflicts, NAMIC advocates that new provisions not be simply a disconnected additional layer of obligations. Rather, to avoid unintended consequences, NAMIC encourages policymakers to consider existing models/laws/regulations. Beyond the privacy space, consulting other resources may be instructive as well. Cautious drafting requires considering existing laws (even those that may not be privacy-specific) to minimize unanticipated compliance conflicts and challenges.

Both the federal and the state data-related regulatory landscape are broader for financial institutions (including insurance companies) than for businesses generally. Consider just a few examples. The federal Fair Credit Reporting Act deals with how consumer reports are handled and the Federal Trade Commission weighed-in with their Affiliate Marketing Rule. Title V of the Gramm-Leach-Bliley Act (GLBA)[2] provides a landmark privacy framework for financial services (including insurance). It sets forth notice requirements and standards for the disclosure of nonpublic personal financial information – it specifically requires giving customers the opportunity to opt-out of certain disclosures. Under GLBA, functional financial institution regulators implemented the privacy standards. Given concerns with consistency, the National Association of Insurance Commissioners (NAIC) unanimously adopted a Model Privacy Regulation. States moved forward with that model.[3] States also have other privacy protections in place today, including protections like those provided as a result of a security breach. Together, these laws are among the many that contribute to the existing significant privacy framework for financial institutions. The existing regime has been working, with processes in place and regulators having authority to address concerns. Contrast this with other business segments outside of the regulated industries.

Given the importance of data in the insurance transaction, historically, policymakers have recognized the important role information plays in insurance and they have allowed for various exemptions for operational and other reasons. There are vital business purposes for insurers to collect, use, and disclose information. For example, see Article IV of the NAIC's Model "Privacy of Consumer Financial and Health Information Regulation" (#672)[4] developed to implement the Gramm-Leach Bliley Act. This Model Regulation appears instructive on types of operational functions to preserve and facilitate. It includes functions being performed on behalf of the insurer. It may also be useful to review the exceptions imbedded into Section

[2] See 15 U.S.C. Sec. 6801 et. seq.

[3] State insurance regulators, through the efforts of the National Association of Insurance Commissioners (NAIC) Privacy Protections (D) Working Group, now are evaluating existing and new privacy requirements.

[4] See NAIC Model MDL-672: https://www.naic.org/store/free/MDL-672.pdf?76

13 of the NAIC's "Insurance Information and Protection Model Act" (#670).[5] In addition, many of these exemptions enable insurance companies to meet consumers' expectations of convenience and ease consistent with insurance companies' contractual obligations to their individual customers.

Imbedded in the existing comprehensive privacy framework for financial services and insurance is a general approach of opt-in for health information and of opt-out for financial information. Practical business function exemptions include: eligibility or underwriting, fraud prevention, and account-servicing or processing type tasks. As drafting continues, NAMIC urges exemptions to resemble today's workable privacy structure that is effective for the regulated insurance industry and for customers of insurance products and services. While NAMIC may support an entity-level insurer exemption for certain activities, which may depend in part on the full picture of the model, please note some data-specific observations. For example, under existing laws, an insurer may have federal and state compliance obligations to use data in a number of ways, including reporting and/or checking against databases for things like: fraud, child support liens, Office of Foreign Assets Control (OFAC) watch list, Medicare/Medicaid reporting/liens, fire-loss reporting to state fire marshals, and theft/salvage claims reporting. These laws support important existing public policy mandates and priorities. Also, the insurance industry is subject to record retention requirements.

While concepts like deletion may sound simple and compelling, they are more complex in practice for insurers. This may be due to several factors. There are legitimate business purposes for retaining data. These reasons may range from claim handling to a matter in litigation to fraud fighting. Also, there may be possible costs and operational challenges in complying with a customer's request to delete personal information when the personal information is used by the business to support insurance eligibility and rating determinations. Identifying and deleting such information may create an undue burden in some situations, such as data that may not be readily accessible given storage in back-up or legacy systems. Insurers are required to follow detailed record retention schedules. They are typically organized by document type, as opposed to by data element. Access to certain business history and other information may help regulators during a market conduct exam or audit situation in which they are confirming compliance to ensure consumer protections.

EXCLUSIVITY – CONTENT & ENFORCEMENT - SINGLE AND CERTAIN STANDARDS

In the draft, Section 19 addresses Regulatory Enforcement and Section 20 outlines a Private Right of Action**.** It is essential to avoid multiple layers of regulation. Regulated entities – and more importantly, consumers – benefit from clear and unambiguous rules. This is especially true for an already highly regulated industry, like insurance (where the Insurance Commissioner often serves as the functional regulator). Possible overlapping and/or inconsistency between privacy/data security requirements may occur when requirements come from various sources: Federal and individual states, legislative and regulatory, functional [insurance] regulator and Attorney General, Judicial interpretations, existing requirements and new mandates, and other standard setting organizations. These evolving and multi-faceted challenges are costly and time consuming for businesses. They may also impact consumers. At a time when most want simplified and efficient communications, these additional – and possibly duplicative – steps may be confusing and require more of a consumer's

[5] See NAIC Model MDL-670: https://www.naic.org/store/free/MDL-670.pdf?92

time to be dedicated to a transaction and/or may impede a business' ability to meet expectations. When more than one agency may engage in rulemaking and/or enforcement, the potential for differing views may mean that financial institutions may be subject simultaneously to potentially inconsistent or conflicting interpretations. Uncertain legal and regulatory requirements make a business environment more costly and unpredictable, at best.

NAMIC may be more supportive of a model that considers the importance of exclusive enforcement without the threat of private litigation. Further, NAMIC may be more supportive of legislation that recognizes the critical information insurers must have in performing functions core to the nature of insurance in protecting people from risks. As stated above, financial institutions (including insurers) are subject to the federal data privacy regulations promulgated under the GLBA, which sets a federal floor that is supplemented by more stringent state laws (that also are applicable to insurers).

In July 2019, the U.S. Chamber Institute for Legal Reform (ILR) published a paper,[6] which examined the resolution of privacy concerns under a variety of different laws. It found problems with the private litigation approach and it concluded: "... privacy statutes that are enforced by government agencies provide a robust process through which noncompliance with protected privacy interests can be identified, remedied, and monitored while promoting consistency, fairness and innovation." NAMIC urges legislators to avoid the pitfalls associated with inviting privacy class actions that largely benefit only lawyers bringing cases for intangible harm. The ILR paper highlights the superior consumer protection of regulator enforcement over a private right of action.

TIMING & EFFECTIVE DATE

Time is important to analyzing these important issues and to drafting provisions carefully. It is also critical for allowing for any guidance to be provided and for subsequent operational changes to be made. NAMIC points to the General Data Protection Regulation (GDPR), which serves as the core of the European Union's legal framework for privacy, as an example not of substance but of process. It replaced the EU's Data Protection Directive, which went into effect in 1995. The GDPR was developed over a long period of time – from 2012 to 2016 when it was finalized – and its goal largely was to enhance an already compatible privacy regime that had been in place for decades. Even then, it allowed for two years before it became effective in May 2018. European Union regulators continue to provide additional guidance and updates to GDPR requirements. Compliance efforts and challenges continue. The more deliberative evolution of GDPR may serve as a template for the timing of these kinds of new approaches. Even within that timeframe, a roll-out period setting forth different dates for different provisions sets-up a more measured approach to undertaking such a significant endeavor. This may be especially crucial for regional or single-state insurers.

When it comes to new laws and regulations on privacy/security, it is important to consider carefully the stability and value of existing laws and regulations and to not act in a way that would confuse and complicate the requirements for those subject to comprehensive oversight today.

[6] https://www.instituteforlegalreform.com/uploads/sites/1/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf

* * * * *

Kindly understand that these comments are preliminary in nature as members assess the draft wording going forward. And, language will continue to evolve in important ways. The practical implications of the operational requirements will depend both on the big picture concepts as well as the specific wording. Because data is essential to an insurer being able to better understand and more accurately underwrite risks, the ability to access necessary information and to comply with other laws regarding information will remain an important component of NAMIC's evaluation of privacy legislation.

NAMIC represents a wide assortment of companies providing valuable services to consumers, and any legislation should account for the different threats these entities face. The existing insurance legal framework relies in part on regulators familiar with the business and operations of different sized insurers within their state market to determine adequate data protections. NAMIC encourages continuing with an approach that is risk-based and scalable. This flexibility may help to ensure that companies have the necessary protections in place to secure consumer data proportionate with its risk and the evolving threat landscape.