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 23, 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. The comments here supplement those NAMIC provided earlier this month and NAMIC may supplement them again as this process moves forward and as members continue their review. Below broad themes are discussed and specific concerns are listed.

GLBA EXEMPTION

Before turning to other discussion, NAMIC again urges a full GLBA exemption in Section 3(b) for all the reasons previously provided.

> (4) a financial institution or any of its affiliated companies that are subject to Title V of the federal Gramm-Leach-Bliley Act (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.

NAMIC urges the Committee to re-frame its GLBA exception in (4) to allow for an ***entity-level approach*** as insurers and other financial institutions should be permitted to use their protection standards across their organization, rather than parsing through individual pieces of data. The way the insurance regulatory process operates, insurers are examined by regulators in Insurance Departments on their enterprise-level controls protecting data, not just around controls that protect specific types of data. This entity level approach for financial institutions, including insurers, would recognize the comprehensive and robust privacy framework in place today under the Gramm-Leach-Bliley Act and other state and federal laws. The National Association of Insurance Commissioners (NAIC) has a working group assembled to review existing laws, regulations, and models applicable to insurers.

PRIVATE RIGHT OF ACTION

A private right of action distracts from the goal of meaningful and real privacy protections where a knowledgeable agency or regulator ensures that businesses is protecting data. Private lawsuits could sweep in technical non-compliance items and it could further erode uniformity. The concept is extremely objectionable. It adds costs to doing business for everyone, including the consumer. NAMIC urges policymakers to avoid the pitfalls associated with inviting privacy class actions that largely benefit only lawyers bringing cases for intangible

[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.

harm. The U.S. Chamber Institute for Legal Reform (ILR) 2019 paper[2] highlights the superior consumer protection of regulator enforcement over a private right of action. 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*."

EXCLUSIVITY – CONTENT & ENFORCEMENT - SINGLE AND CERTAIN STANDARDS

For an already highly regulated industry, like insurance (where the Insurance Department serves as the functional regulator), it is essential to avoid multiple layers of regulation (as would be built though Section 19). Uncertain legal and regulatory requirements make a business environment more costly and unpredictable, at best. Possible overlapping and/or inconsistency between privacy/data security requirements may occur when requirements come from a variety of sources such as: 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. When more than one agency may engage in rulemaking and/or enforcement, the potential for divergent views may mean financial institutions could be subject to inconsistent or conflicting interpretations. At a time when many consumers call for simplified and efficient communications, additional – and possibly duplicative – steps may be confusing and require more of a consumer's time to be dedicated to a transaction and/or may impede a business' ability to meet consumer expectations. Consumers and regulated businesses benefit from clear and unambiguous rules.

TIMING & EFFECTIVE DATE

NAMIC underscores the need for delayed implementation following any regulatory guidance in order for operational changes to be made. The timing of General Data Protection Regulation (GDPR), which forms the core of the European Union's legal framework for privacy, provides a useful example. Replacing the EU's Data Protection Directive, which went into effect in 1995, GDPR was developed from 2012 to 2016 when it was finalized. Then, it allowed for two years before it became effective.

OBSERVATIONS

The notes below reflect some additional issues and challenges members identified with the draft.

- Members are continuing to review the different approach taken in the ***definitions***. They identified several questions and concerns. For example, because of the nature of the business the language relative to *profiling* and *automated decision-making* should specifically *exclude* insurance underwriting and rating. The inclusion of "physical location," "movements," "behavior" seems particularly problematic. Also, being able to identity personal information within a household or device may be difficult. Additionally, the requirement that a business reasonably prevent the "inadvertent release" of de-identification is unclear.

- In addition to the GLBA exception revision highlighted above, members shared several other remarks on the draft's ***scope*** section. The "scope" criteria in (a) would be clearer if it states that the only individuals that count, in terms of determining whether a threshold has been met, are those residing in the specific state. Also, the employee exemption should be expanded to add former employees, temps, applicants, contractors and beneficiaries. The Model would also benefit from a business-to-business exemption to carve out individuals who provide information in the context of a commercial transaction between businesses. The term "publicly available" in (b) should be expanded to include information readily available on the internet. Subsection (c)(4) would benefit from

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

additional language the effect that this particular law will not impact the ability *to assert* a claim. As drafted, it indicates only defending a claim.

- The draft Model appears to consider "***data subjects***" to be a device or a household. The household designation approach is problematic because a household is not static. For example, one day it includes a roommate or boyfriend, the next day it does not. As a practical matter, how is a company to track that and be sure to only disclose data to the right people? To consider a device to be a data subject is also questionable. Data subjects are traditionally categories of people. For example, employees or claimants would be considered data subjects (but not devices).

- A number of practical operational items are raised when it comes to ***accessing, correcting and deleting*** information. Deletion requests should be limited by some practical exceptions. The right to correct inaccuracies should be limited to correction of inaccuracies that affect the consumer. While there is a limitation on providing the data held by a business in response to a valid customer request to one time per year (though it could be clearer that it is one time per year, not one time per year for no charge), there is not a limit to the number of times that a customer can check with a business to confirm whether the controller has retained or is processing the data subject's personal data under Section 4. Section 5 limitations are only in place for requests for personal data.

- It appears that the draft is structured to require a way to opt out of ***targeted ads*** (something like a cookie preference center) would need to be implemented. This would be a problematic – the technology to do so does not appear to be readily available.

- In Section 6, the ability to opt-out of "***profiling***" should exclude insurance rating and underwriting. The application of an opt out for "profiling" in Section 6(a)(2) appears to be too broad and may infringe upon normal rating and underwriting of insurance. Historically, risk underwriting or rating model output information has not been provided to individuals in the form contemplated under the draft. Issues around the possible consequences of the profiling definition and wording are of concern. For example, Section 3(c) provides that "nothing in this act shall prevent the collection, authentication, maintenance, retention, disclosure, sale, processing, communication, or use of personal information necessary to complete a transaction in goods or services that the data subject requested." This contemplates a transaction was already initiated. In Section 17, as long as there is not discrimination because a data subject requested their data or requested corrections to their data, "a data controller may adopt and enforce as a condition for access to its good or services that consumers permit the processing of their personal data." A question has been asked whether it is sufficiently clear that the profiling may occur at a point before a contract is signed and whether notice in the privacy policy (online) is sufficient for "adoption and enforcement." As a practical matter, these issues may be important for quoting.

- While it makes sense to have ***privacy commitments*** on the website, filing with the AG seems unnecessary. In addition, the "uniformity" of the law is undercut by 50 potentially different Administrative Procedure Acts in each state for enforcement.

- The ***loyalty*** set forth in Section 9 section is troubling as it may set-up new causes of action. For example, as drafted, a business could provide a detailed privacy notice to a consumer telling her before collecting data that it will collect these data points and use them in certain ways. If subsequently a plaintiff's lawyer thinks that the use of the data as described in the notice may result in unreasonable harm to the individual, the business may be considered to have breached a "duty of loyalty." This is counterintuitive – the point of a privacy notice is transparency. It gives the individual the right to choose those with whom she does business. It is unfair for the consumer to be provided the opportunity to make that informed choice and then later assert the very disclosed use of data is a breach of loyalty. Adoption of fair information principles should reside in the privacy notice; this overlaps with the existing laws of some states. An unfair practice is generally known as a practice that subjects the data subject to an unreasonable material risk of harm. The model does not reference a standardized risk framework. This again points to opportunity for inconsistency: each

state Attorney's General may have different methodologies to determine what constitutes material harm and then the door appears to open for civil suit.

- In reviewing the Section 10 draft ***data security*** obligations, the wording indicates that "An evaluation of the reasonableness of data security measures shall take into consideration the magnitude and likelihood of security risks and potential resulting harms, the resources available to the custodian, and industry practices among other custodians who are similarly situated. Reasonable security practices may be derived from best practices promulgated by professional organizations, government entities, or other specialized sources." While it is beneficial to balance flexibility and some certainty. As drafted, it does not appear that this would be uniform, additional discussion of a standards may prove helpful.

- The ***data minimization*** responsibilities in Section 11 could create inflexibility.

- As drafted the ***purpose limitation*** in Section 13 could introduce endless debates around technicalities. It seems appropriate for the wording to indicate that in order to be triggered, the purpose not specified would need to differ materially.

- The wording in Section 14 automatically makes the ***processing*** of personal data (as broadly defined) without a written agreement "unfair act" which would be subject to enforcement and to possible private litigation. This could be extremely problematic as it does not contemplate certain situations. Data may be processed, under number of circumstances, in the absence of a written agreement. For example, consider data sent to the National Insurance Crime Bureau (NICB) or to a third party pursuant to consent.

- The ***Data Privacy Officer*** designation requirements in Section 15 should be revised to consider some important operational items. For example, it may be that each individual entity within an enterprise should not need to designate separately. Also, consider whether there should be a threshold requirement for DPOs based on the size of the company and the magnitude/sensitivity of the data processed.

- The ***Privacy Impact Assessments*** in Section 16 appear overbroad and unduly burdensome. The obligation to develop a *very detailed* privacy assessment could be burdensome. The requirement to evaluate all potential harms to data subjects could be difficult, in particular without appropriate and reasonable standards. It does not appear to fully appreciate the need for flexibility in an approach that is risk-based and scalable. Even under GDPR, PIAs are required only for the processing that constitutes the highest risk to privacy. They are not required for "all processing." With a broad processing definition that includes storing, access, use, transfer, etc., as the trigger, the number of PIAs a company would have to complete is mind boggling. For example, one member conveyed that for just one line of business an insurer might have hundreds of PIAs. Procedurally, this section also appears burdensome. The assessments would need to be updated every two years and apparently signed personally by the DPO. These assessments should be required and updated based upon risk, not based upon a blanket approach. Further, PIAs are used for internal risk assessments and should be permitted to be done under applicable privilege. A mandate to disclose them to the Attorney General's office (again, not a functional regulator) undermines allowing the company to look critically at its risks and to document mitigation. Importantly, consider the possible damage if for some reason the documents are released and this sensitive information lands in the hands of hackers.

* * * * *

As members assess draft wording and future modifications, NAMIC may further supplement our comments. Thank you.