NAMIC® ADVOCACY

CCPA: A MODEL TO FOLLOW OR AVOID?
QUESTIONS TO CONSIDER

CATE PAOLINO
Director of Public Policy
National Association of Mutual Insurance Companies

NAMIC®
ISSUE ANALYSIS

CATE PAOLINO

Cate Paolino serves as NAMIC's Director of Public Policy. She is responsible for providing the association and its membership with key policy expertise and analysis on legislative and regulatory issues of interest to the property/casualty insurance industry at the state, federal, and international levels.

Paolino is a former NAMIC Regional Vice President of the Northeast Region. She came to NAMIC from Travelers, where she worked in business insurance serving as senior counsel and second vice president, Regulatory Research and Compliance. She spent more than 10 years as senior counsel at the American Insurance Association. Her skill set includes legislative and regulatory analysis, legislative drafting including the drafting of model legislation, experience with commercial insurance issues and drafting and presenting testimony.

She holds an MBA from Suffolk University and a law degree from the University of Connecticut.

For more information about this NAMIC Issue Analysis please visit www.namic.org/issues/our-positions or contact:

Cate Paolino
cpaolino@namic.org
508.431.0484

NAMIC membership includes more than 1,400 member companies. The association supports regional and local mutual insurance companies on main streets across America and many of the country's largest national insurers. NAMIC member companies write $268 billion in annual premiums. Our members account for 59 percent of homeowners, 46 percent of automobile, and 29 percent of the business insurance markets.

TABLE OF CONTENTS

Consumer data security and privacy protections have been a long-standing and top concern for insurance companies. Recently, there has been a flurry of activity in the privacy space, with the most widely discussed efforts happening in California.

This paper provides a brief consideration of the California Consumer Privacy Act from an insurance industry perspective. It is not intended to address the nuts and bolts of specific requirements needed for compliance or implementation, but instead to raise several important questions and issues to provide a context for discussions of whether it is timely for other states to consider CCPA as a model for their privacy framework.

WHAT IS CCPA?

The California Consumer Privacy Act of 2018,[1] effective as of January 1, 2020, is generally described as creating five new consumer rights. They include the right to:

- Notice of categories of personal information collected and purposes for that collection;
- Access to additional disclosure generally and consumer-specific pieces of information;
- Deletion of personal information not falling into an exception;
- Opt-Out of the sale of personal information and an opt-in by a minor's guardian; and
- Nondiscrimination from different treatment, if exercising a CCPA right to restrict downstream sale of information and in some other situations.

Without minimizing the significance of the law, it is useful to consider these CCPA obligations from the perspective of existing situations in which businesses: (1) give mandatory notice/disclosure; and (2) make available optional elections. This framing sets the stage for discussing data-related mandates, choices, and restrictions as being on a continuum, which helps center the conversation around factors such as whether a proposed regulation is optimal for insurance consumers. One could easily imagine a circumstance in which consumers are so inundated by formal wording describing their various options regarding data collection and/or use that they simply choose to opt-out of everything, thereby denying themselves the benefits of constructive uses of their data.

Under CCPA, consumers need to be provided information about data collection and use at different stages of their relationship with a business. For example, an insurer would need to follow specific timelines to inform consumers about categories of personal information collected with specifics available upon request; source(s) of that data; uses of such collection and categories; whether the information was disclosed or sold to third parties; categories of personal information disclosed or sold to third parties; and categories of third parties to whom such information was disclosed. Some of these categories of personal information defined by CCPA may not mesh easily with current disclosure requirements under other state and federal laws. And these notices would be provided in addition to or in conjunction with privacy notices already required by those laws. (See Gramm-Leach-Bliley Act discussion.)

Some practical questions are worth considering. First, is this simply too much information for an average consumer? Similarly, does that consumer even want to sort through details beyond whether personal information is being sold or used for unanticipated purposes? Under CCPA, consumers must be given access to personal information that has been collected during the 12 months prior to the request. How important is an access report to the typical insurance consumer? And at what cost? How many insurance consumers would voluntarily agree to pay more in premiums for this type of access report?

WHY IS CCPA CONSIDERED AN UNFINISHED MOVING TARGET?

When the CCPA was passed in 2018, it moved very swiftly. Since that time, there has been a great deal of confusion and concern, as well as a good deal of activity that has further complicated the issue.

Among those complicating developments are a multitude of bills introduced to revise the law as originally passed. Indeed, several bills amending the CCPA were enacted in 2019.[2] Those amendments span a wide range of changes, from definitions to authentication and from biometric data to record retention, among others. Some legislators have already indicated they have plans to move forward with legislative efforts to further amend CCPA in 2020.

In addition, as of the date of this paper's publication, the original law's implementing regulations still have not been finalized. The California attorney general disseminated proposed regulations in October 2019 to govern compliance with the CCPA. The regulations focused on several practical items that have yet to be finalized, including consumer notifications, handling opt-out requests, and verifying identities. Public hearings were held, and comments were due on the attorney general's first proposal in December 2019. Modified proposed regulations were posted for written comment in February 2020.

Even after final promulgation, these regulations may not be the end of the changes to the California privacy landscape. With what some are calling "CCPA 2.0," efforts are underway with a ballot initiative, "The California Privacy Rights and Enforcement Act of 2020," which would expand the CCPA in several respects. The initiative itself has also been unstable – with new text replacing what was first published. From all this activity, it appears that the California privacy requirements are unclear today and will continue to be well into the future. NAMIC is currently urging other states not to attempt to mimic or modify this unsettled California privacy environment.

WHAT INSURANCE-RELATED PRIVACY PROTECTIONS ARE IN PLACE TODAY?

Existing laws and regulations already address privacy protections for insurance consumers. Both the federal and the state data-related regulatory landscapes are broader for financial institutions than for businesses generally. Consider just a few examples. The federal Fair Credit Reporting Act addresses how consumer reports are handled and the Federal Trade Commission weighed-in with its Affiliate Marketing Rule. States also have their own privacy protections in place today, including protections provided as a result of a security breach.

Title V of the Gramm-Leach-Bliley Act provides a privacy framework for financial services, including insurance. It sets forth notice requirements and standards for the disclosure of nonpublic personal financial information, and it specifically requires giving customers the opportunity to opt-out of certain disclosures. Importantly, GLBA allows for functional financial institution regulators to implement the privacy standards. Given concerns with consistency, the National Association of Insurance Commissioners unanimously adopted a Model Privacy Regulation, and states have moved forward with that model.

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 large internet and technology companies, which are largely outside the regulated industries discussed in this paper and are generally considered the targets of CCPA.

WHY ARE NEW PRIVACY REQUIREMENTS LIKE CCPA OF CONCERN TO INSURERS IF THEY ALREADY HAVE PROTECTIONS IN PLACE TODAY?

As the scope of laws/regulations change, the analysis and impact change, too. Consider the many ways laws may vary from jurisdiction to jurisdiction and may change over time, examples include the definition of "personal information" or details on how a new one-size-fits-all mandatory method to categorize, communicate, and/or interface is structured. When laws and regulations change, businesses must review information and processes through a different lens, distinct from the previous requirements in a way that may not be consistent with its existing comprehensive data map or in vendor contracts, both of which may have undergone recent changes due to previous legislative/regulatory requirements or updates.

First, consider the operational implications. In general, new and different requirements add another layer to the obligation to review information, its sources, and methods for its handling. For property/casualty insurers, this may be across many components, including:

- Products – Lines of business and types of insurance;
- Systems – Divisions within an enterprise, either by function or by older legacy companies/subsidiaries and newer technology;
- Party and Purpose – Restrictions exist for affiliate sharing and affiliate marketing; and
- Distribution Channels – Direct online or mobile, independent agency, or affinity programs.

Second, consider the possibility of overlapping and/or inconsistency between privacy and data security requirements. Additional levels of layering may occur from various sources:

- Federal and individual state governments;
- Legislative and regulatory;
- Insurance regulator and attorney general;
- Judicial interpretations through private actions;
- Existing requirements and new mandates; and
- Other standard-setting organizations.

This evolving and multi-faceted analysis is costly and time consuming for businesses and may also impact consumers. At a time most want simplified and efficient communications, these additional – and possibly duplicative – steps may be confusing and may require more of a consumer's time to be dedicated to a transaction and/or may impede a business's ability to meet expectations.

WHAT ARE SOME POSSIBLE UNINTENDED CONSEQUENCES OF A LAW LIKE CCPA FOR FINANCIAL SERVICES COMPANIES AND CUSTOMERS?

When considering imposing new standards, policymakers are well served in taking a wider view of possible conflicts and/or unintended consequences.

- Under existing laws, an insurance company may have federal and state compliance obligations to use data in a number of ways, including reporting and/or checking against databases for information that may help alert or inform in instances such as:
    - Fraud;
    - Child support liens;
    - Office of Foreign Assets Control 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 consider that the insurance industry is subject to record retention requirements.
- Overbroad or rushed measures may be expensive, result in duplicative compliance costs, increase litigation, and/or impact consumers negatively.
- Generally, in today's market, consumers demand streamlined decisions and products. They want quicker service with less manual data entry. All parties benefit when policymakers use care not to restrict the ways insurers may innovate to understand risks and/or to respond to these consumer demands.

WHAT IS "GDPR" AND HOW DOES IT RELATE TO CCPA?

The General Data Protection Regulation serves as the core of the European Union's legal framework for privacy. It replaced the EU's Data Protection Directive, which went into effect in 1995. The GDPR attempts to provide a single set of uniform rules/standards (and a single supervisor authority within the EU member states) regarding personal data for those with data processing activities that relate to offering goods or services to individuals in the EU or to monitoring the behavior of such individuals. While CCPA differs from GDPR, the primary focus of GDPR may also be distilled to giving certain disclosures and to making certain options available.

The GDPR was developed over a long period of time – from 2012 to 2016 – and its goal was largely 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. EU regulators continue to provide additional guidance and updates to GDPR requirements. Compliance efforts and challenges continue. By contrast, and as a practical matter, CCPA imposed sweeping changes to the privacy landscape in California with little time for businesses and regulators to prepare. At the very least, the more deliberative evolution of GDPR may serve as a template for the timing of these kinds of new approaches.

WHEN IT COMES TO STATES CONSIDERING NEW LAWS AND REGULATIONS ON PRIVACY/SECURITY, WHAT CONCEPTS SHOULD BE CONSIDERED?

Legislative and regulatory considerations of privacy regulations should involve careful consideration of the stability and value of existing laws and regulations and not acting hastily in a way that would confuse and complicate the requirements for those subject to comprehensive oversight today. Turning to several foundational concepts for a legal/regulatory privacy framework for insurance will be essential for policymakers:

Workability – Historically, insurance 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)[3] developed to implement the GLBA. This model regulation appears instructive on types of operational functions to preserve and facilitate. It may also be useful to review the exceptions imbedded into Section 13 of the NAIC's "Insurance Information and Protection Model Act" (#670).[4] 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 customers. Clear and well-crafted provisions accounting for GLBA and FCRA are important in any broader business legislation.

Exclusivity – It is essential to avoid dual regulation. Regulated entities and, more importantly, consumers benefit from clear and unambiguous rules. As discussed in the question regarding why new requirements are cause for concern, 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.

Clarity – New provisions would not be enacted in a vacuum. 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, new provisions should not be simply a disconnected additional layer of obligations. Rather, to avoid the unintended consequences discussed in this paper, policymakers must consider how best to dovetail new laws with existing models/laws/regulations. Consulting other resources may be instructive as well. Today, laws may require insurers to use data to advance public policy objectives, including reporting and/or checking against databases. Cautious drafting requires considering existing laws, even those that may not be privacy-specific, to minimize unanticipated compliance conflicts and challenges. Building in enough time for each stage – analyzing, drafting, reviewing, deliberating, rulemaking, implementing – is crucial.

Effective Date – Time is needed not only to analyze the issues and draft provisions carefully, but also to allow for any guidance to be provided and for subsequent operational changes to be made. While there is much discussion of the California law, even if a state decides that some CCPA provisions merit inclusion in its jurisdiction's laws, it is unfair to assume that insurers may be ready to implement that approach in the near term. Some regional or single-state insurers may not do business in California; their practices today may not be built around that state's law. And as previously mentioned, the California approach remains a moving target. The complexity of the potential changes necessitates delayed implementation and guidance consistent with the law throughout the implementation process to facilitate compliance. Specifically, a timeline should be similar to the two to five years afforded under GDPR. Even within that time frame, a roll-out period setting forth different dates for different provisions sets up a more measured approach to undertaking such a significant endeavor.

SHOULD OTHER STATES MIMIC THE CALIFORNIA APPROACH?

States would be best served by deferring the decision of whether to move forward with legislation similar to the California approach until it is truly final – with amendments and pending bills completed, regulations finalized, initiatives behind us, and with time to see any implications of that implementation – and until the challenges and unintended consequences of the California approach can be better cataloged and understood.

State insurance regulators are in the process of reviewing the steps California has taken, through the efforts of the NAIC's Privacy Protections (D) Working Group, which is evaluating existing and new privacy requirements. Its workplan includes possible drafting of model wording "to address appropriate insurance privacy protections regarding the collection, use and disclosure of information gathered in connection with insurance transactions" by the NAIC's 2020 Summer National Meeting.

In short, other states have a real opportunity to learn from the California experience before they rush forward with laws that duplicate this still "unfinished moving target." One lesson already learned is that it is extremely important for policymakers to allow for adequate advance time for businesses to prepare for an effective date. No doubt, there are more lessons to be learned for other states that pause to fully understand the final content and consequences of CCPA.

ENDNOTES

[1.] See Assembly Bill 375 (2018).

[2.] See Assembly Bills 25, 874, 1130, 1146, 1355, and 1564.

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

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

NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

3601 Vincennes Road | Indianapolis, IN 46268 | 317.875.5250
20 F Street, NW, Suite 510 | Washington, D.C. 20001 | 202.628.1558

NAMIC

NATIONAL ASSOCIATION OF
MUTUAL INSURANCE COMPANIES