2021 Annual Conference
June 16-18, 2021
Atlanta, Georgia

A Heavy (and Expensive) Burden: Managing Data in the Age of Data Privacy Legislation

I. INTRODUCTION

In a world focused on speed, we need to take a time out. Our ability to store, manage and transmit information geometrically increases every year. Our identities from likeness to medical and financial information are transmitted without forethought. In response to the speed and proclivity of others to leverage personal information for financial gain, governments abroad and in the United States began to address the key protections necessary to have a secure identity. This movement is fueled by the security of privacy and choice for use of personal information.

II. COMING TO AMERICA

When the European Union (EU) adopted the General Data Protection Regulation (GDPR) in 2016, it foreshadowed a new standard which spread to other countries including the United States. This, in turn, attracted the attention of state legislatures. Given the EU's GDPR implementation period which ended May 25, 2018, many businesses, individuals, and entities of all types adjusted to this new reality. It placed new responsibilities onto the holders of information. This geometrically increased responsibility for successful compliance and pro-active management of its attendant risk.

GDPR attached for any global business which had EU customers. This brought the focus to other countries, including the United States.

When GDPR focused on "any information relating to an identified or identifiable employee" in personal data, it did not parse out or differentiate. It was a classic example of when less meant more.

It was not only what was in a name, but also other identifiers such as:

1. Address for home and work
2. Birth data
3. Car ownership/usage including license plate or vehicle identification number

4. Chauffer's or Driver's license information
5. Credit information
6. Disability(s)
7. Email addresses
8. Educational history
9. Ethnic origin
10. Health issues including medical and mental health records
11. Investment and/or retirement accounts
12. Job description, performance, and reviews
13. Legal histories including criminal and litigation searches
14. Media usage and related account information
15. Mobile communications and wearable devices
16. Passport data and travel history
17. Philosophical and/or religious beliefs
18. Sexual identity and gender preferences

Given personal information transfer for-profit and harvesting for nefarious activity, placing the burden on the holder created new legal, social, and community responsibility.

III. CALIFORNIA HERE WE COME

Not surprisingly, California moved into the forefront with the California Consumer Privacy Act of 2018 (CCPA). This law, which goes into effect on January 1, 2020, is an extension of protection for individuals for the retention and use of personal information. It broadly defines the consumer, creates the right to know what is done with the information. It includes the right to access, delete, and opt-out of sharing.

In addition to relief that can be sought by the Attorney General of California, it also creates a private cause of action. Those protected by the law can enforce their rights in court, seek statutory damages and injunctive relief. It raises the risk to holders of information that theft, unauthorized disclosure, and failure to maintain security procedures can give rise to monetary damages. A potential vehicle for such private lawsuits may eventually involve class actions to maximize recoveries.

Recent attempts to cushion the implementation of CCPA have resulted in amendments that extend implementation on employee data where they are acting on behalf of a business entity. It also created an exemption for the Fair Credit Reporting Act for use of consumer credit information for a consumer reporting agency. Recent amendments to the law go into effect on January 1, 2022, and regulations will continue to be refined during 2021.

A summary of the basic requirements is in order. First, unlike GDPR, the CCPA applies to for-profit companies only (as opposed to non-profits). Application of CCPA applies if one of the three following factors are met:

1. Annual gross revenue of greater than $25 million;
2. Information of 50,000 or more people which also counts devices; or,
3. 50% of revenue from the sale of personal information.

Personal information is defined more broadly than GDPR and includes, for example, households, profiles, biometric information, geolocation data, professional and education data over and above the earlier list. Stakeholders need to carefully consider the definitions of personal information as they may vary from statute to statute and state to state. In short, it only treats very few other sources, as different, such as information protected under the Health Insurance Portability and Accountability Act of 1996 (HIPPA).

Some key provisions focus on informing consumers, limiting collection and use, providing an opt-out option, providing under limited circumstances an opt-in for certain minors, requires privacy notices, ensure the ability to delete personal information, require that consumers are not discriminated against if they exercise their rights and to take reasonable security precautions to protect personal data.

Businesses will be required to have, on their website, an option or link for the consumer not to allow the use of their personal information. This creates a higher profile for the exercise of the right of privacy for the consumer and for the business to know whether or not one elects to make their information private or not.

The penalties are significant. For data breaches, it is $7,500 per violation. For other breaches, it is $2,500 per violation. As noted earlier, there is an individual right of action. For those individual rights of action, there is a $100 to $750 standard per breach. Unlike GDPR, which caps liability at 4% of global revenue or 20 million euros, there is no limit under CCPA. This creates a geometrical exposure for non-compliance.

IV. CCPA EXPANSION SLOWED IN OTHER STATES

Other states started down the path of CCPA. Legislation considered in 2020 seeks to extend a similar CCPA model to Massachusetts, New York, Hawaii, and Maryland. Other states are considering further action as well.

For example, in Illinois, the Data Transparency and Privacy Act was introduced, sailed through the Assembly with enforcement reserved to the Attorney General of Illinois. It was later amended which raised the specter of private causes of action with potential class treatment. This resulted in the bill stalling without approval. In the State of Washington, the Washington Privacy Act sailed through the state Senate but failed to pass in the Assembly. It was reintroduced in January 2021

The Texas Privacy Protection Act did pass and was signed into law by Governor Abbott which created a 15 member Texas Privacy Protection Advisory Council to issue a report to state privacy laws by September 1, 2020 (as the Texas legislature meets every other year). Nevada adopted a “skinny” version of CCPA which focuses on the sale of information. Other states appear on the march for the adoption of similar new laws in 2021.

V. READ WITH OTHER CONSUMER PRIVACY LAWS

In Illinois, the Biometric Information Privacy Act (740 Ill. Comp. Stat 14 2008) focuses on fingerprints, voiceprints, retina or iris scans The Act, which has been in effect for 10 years, requires companies to inform individuals the purpose of collection, length of time for storage and use, provide a written policy for retention and a release from the individual before collecting and sharing with a third party.

The BIPA provides for enforcement including a private right of action. In the recent decision of Rosenbach v. Six Flags Entertainment Corporation 2019 IL.123186, 129 N.E. 3rd 1197, the Illinois Supreme Court determined that a plaintiff need not suffer actual harm to have the standing to sue. As such, traditional forms of damage, such as injury, in fact, that results in economic loss or some other tangible injury is not required

This foreshadows potential future treatment under the new wave of consumer protection statutes. Since actual harm is always difficult to prove, a right of action without traditional causation and damage will likely create a stronger capacity for enforcement. It also creates greater exposure to businesses and all stakeholders for non-compliance.

VI. NEED FOR FEDERAL LEGISLATION

As a large state which borders Oregon to the north, Nevada and
Arizona to the east, the CCPA presents quite a challenge for contiguous states and those who assemble goods and services through multiple states that include California. Efforts at legislation at the national level have not met with success with attention divided into multiple issues. Ultimately, like the EU which has 28 countries, the United States has 50 separate states each of which has a connection to the world's 5th largest economy: California.

Ultimately, for many, the ability to simultaneously comply with different requirements among the states will lead to confusion, duplication, and potential non-compliance by error or omission. Congress may consider such legislation in furtherance of the Commerce Clause. U.S. Const. Art. 1, Cl. 8. Such legislation would likely supplant multiple, conflicting laws through U.S. Const. Art. VI, Cl. 2 as: "…the supreme law of the land."

Much in the same way the Health Insurance Portability and Accountability Act (HIPPA) introduced greater privacy requirements in health care, the Congress and President are likely to review privacy in the consumer protection context in the next few years.

VII. WHAT SHOULD WE DO NOW?

To quote Flight Director Gene Kranz from the movie Apollo 13:
"…failure is not an option." Neither is ignoring the law and hoping that you don't get caught. So, what are businesses, including insurance companies, third-party administrators, insurance brokers, general counsel for companies, and risk managers to do?

First, review what you already have. Like the merchant at year's end, do an inventory. What type of information do you have? Why do you have it? How do you use it? How do you protect it? It is likely that most have some measures in place, but here are a few which should be considered: anti-virus software, database design security, filters for emails, firewalls,

planning for network usage which includes monitoring, user access controls, web access/filtering, and common sense. We live in a world where a data breach is not possible, but probable. Planning to succeed can work, not planning at all is planning to fail.

Second, review your information technology policies which include security, continuity, and recovery plans. Design and implement controls. Train staff and promote greater awareness through scheduled refresher training. Follow updates and the latest developments in technology. Have a "dry run intrusion" event to check your system and see how your staff follows the protocols established. It may sound like a fire drill, but if you train your staff on how to get out of a building, they should be able to respond to an event that potentially threatens personal information you maintain.

Third, engage in enterprise risk management generally, and with the compliance of CCPA and similar laws, in particular. Engage management at all levels, including the "C Suite," so everyone is on board. It is also important that any third parties, such as vendors and service providers, have at least the same level of concern for and security of personal information. Try to ensure that you do business with companies and individuals who have a likeness to yours for the seriousness of this endeavor.

Fourth, review and update your insurance coverage to encompass risk transfer in the event of the probability, not the possibility, of a data breach. It is amazing that many stakeholders, including some who attend CLM events, do not have cyber coverage. It is still reasonably affordable. Such coverage has a 1st party component to respond in the event of a breach and a 3rd party component to address liability.

Other potential sources of risk transfer may be contained in commercial liability, directors and officer's liability, fidelity, professional liability, and other coverages. Finally, contractual responsibilities through indemnity and additional insured protection with third parties and vendors should also be explored.

VIII. INSURERS AND BROKERS HAVE RESPONSIBILITIES

While GDPR has applied to the insurance industry already and CCPA
arrives on New Year's Day, insurers, brokers, and others involved in the business already have responsibilities to meet which cannot be ignored. Insurers and brokers possess a treasure trove of personal information.

In November of 2017, the National Association of Insurance Commissioners (NAIC) adopted the Data Security Model Law (DSML). This tracks many features of HIPPA and the New York State Department of Financial Services regulations, and, in particular, 23 New York Codes Rules and Regulations 500. While this model law has not been adopted in all states, it is likely, like consumer privacy laws, to be extended throughout the nation.

This extends to licensees which may include insurance brokers in many offices. It does except those licensees with fewer than 10 employees. It does have certain requirements all stakeholders should be aware of, which include, but are not limited to:

1. Licensees should have a written Information Security Program;
2. Non-public information is protected. This goes beyond personal information to include business information.

As each state which had adopted its own version of the DSML, and they differ to some degree, stakeholders need to be familiar with those laws applicable to their business. At present, the following states have adopted some form: Alabama, Connecticut, Delaware, New Hampshire, Ohio, and South Carolina.

IX. CONCLUSION

Like the clientele we serve, stakeholders in the insurance industry need to navigate on the sea of perpetual change. In the present environment with a reduction in the significance of international and state borders for the protection of personal information, we need to develop a mindset to accept the challenge of perpetual change. Those who can adapt have a greater advantage in the marketplace and will have a stronger brand.

With the advent of a return to greater privacy through respect for the choice of the individual, the wisest course is to adopt compliance with the most stringent set of privacy laws and thereby subsume the ability to address others with greater ease. Nuances will not disappear; however, will be much easier to address in a context of comprehensive preparation.

So our panel concludes with simple advice. Imagine it was you. How would you like to be treated, have your preferences respected, and your information protected? Perhaps, in the endless world of complexity, a Golden Rule of Personal Privacy is the advent for the new decade.

Respectfully submitted,

Howard Franco, Jr., Partner
Collins Collins Muir + Stewart, LLP, Carlsbad, California

Lisa Jaffee, Esq., Assistant Vice-President of GB Specialty/
Western Litigation, New York, New York

Laura Zaroski, Esq., Managing Director
Gallagher Law Firm Group, Chicago, Illinois

Yosha De Long, Sr. Vice-President
Global Head of Cyber Underwriting
Mosaic Insurance Company, Chicago, Illinois