O'NEILCANNON
HOLLMAN DEJONG & LAING S.C.

OVERVIEW OF DATA PROTECTION LAWS IN WISCONSIN

Almost every organization in the world collects personal data from individuals, in one form or another. Indeed, most websites collect consumer information automatically. For this reason, every business must become familiar with relevant data protection laws and understand how to collect, store, use, and share data in compliance with these laws. Organizations that fail to comply with data privacy laws could incur substantial fines and other damaging consequences.

This blog post intends to give Wisconsin organizations a basic overview of consumer data privacy laws, their significance, and how such laws may apply to them.

What is Privacy Law?

"Privacy law" refers to laws governing the regulation, storage, sharing, and use of personally identifiable information, personal healthcare information, financial information, and other types of personal information. While both state and federal governments have various laws governing certain types of information privacy, as of now, no federal law exists to protect consumer data.

Given the absence of federal protection and the number of internet companies collecting—and often misusing—consumer data, several states, including Wisconsin, have developed or are beginning to develop state statutes designed to protect residents from data misuse online. Together with international data protection regulations, these state laws create an increasingly complex web of obligations for any organization collecting personal data.

What is Personally Identifiable Information?

The key to understanding and properly complying with consumer data privacy laws is understanding the term "Personally Identifiable Information" (PII). In general, PII is any information that may be used to identify an individual. Such information may include not only names, addresses, and government IDs, but also internet protocol (IP) addresses, cookie identifiers, and other automated identifiers.

Despite their many commonalities, international and domestic privacy laws have subtle differences in their categorization of PII. For example, some privacy laws allow pseudonymized or anonymized data to be excluded from PII. Pseudonymization is a reversible process that substitutes the original personal information with an alias or pseudonym such that additional information is required to re-identify the data subject. In contrast, anonymization irreversibly eliminates all ways of identifying the data subject. Similarly, IP addresses may be either static (i.e., specific to a particular computing device) or dynamic (i.e., the IP address changes over time). Static IP addresses are likely to be considered PII whereas dynamic IP addresses may not, depending on the applicable law.

An Overview of Key Data Protection Laws

Modern consumer data protection laws generally articulate both consumers' rights to data privacy and the responsibilities of entities that collect and process personal data.

Concerning consumers, most consumer data privacy laws establish that consumers have any combination of five fundamental rights, including the right to:

- be informed that data is being collected;
- access collected data;
- rectify incorrect data;
- erase collected data; and
- object to certain uses of that data.

While these diverse privacy regimes have many similarities, they often have substantial differences, including varying definitions, scope, punishment for violations, and jurisdiction. Therefore, it's critical to determine which laws apply to you and to thoroughly review those laws to understand your organization's compliance obligations.

a. The European Union–General Data Protection Regulation (GDPR)

The European Union's (EU) data protection regulation, known as the GDPR, is the world's first comprehensive data protection law. Having gone into effect in 2018, the GDPR interprets PII extremely broadly and takes substantial steps to protect such PII. It covers not only IP addresses and cookies but also certain forms of pseudonymized data and metadata. The law is revolutionary in that it applies to all entities possessing or processing the personal data of EU residents, regardless of an entity's nationality. Therefore, U.S. companies who deal with EU citizens as customers, users, or clients are likely to be subject to GDPR rules and regulations.

It is crucial to determine whether your organization is subject to GDPR rules. Should EU regulators determine that a company subject to the GDPR has violated any of the GDPR articles, the company may be subject to fines for as much as €20 million or 4% of the

company’s global turnover, whichever is higher.

b. The California Consumer Privacy Act (CCPA)

Effective as of January 1, 2020, the CCPA is the first significant consumer data protection act in the United States. Like the GDPR, the CCPA defines PII to include any information that could, directly or indirectly, lead to the identification of any user or household.

Also similar to the GDPR, the CCPA is applied broadly to businesses globally should they do business in California. The CCPA includes specific language defining what businesses are subject to the CCPA. The CCPA applies to any for-profit business that collects, possesses, or otherwise handles the PII of California residents AND that meets any of the following criteria:

1) has annual revenues over $25 million;

2) possesses the personal information of 50,000 or more California consumers, households, or devices in any calendar year; OR

3) earns more than half of its annual revenue from selling consumers’ PII.

This statute is intended to be broadly applied to commercial enterprises, regardless of geographical location and whether they explicitly target California residents. Because most businesses operate websites that automatically collect PII, such as cookies or IP addresses, even small non-California businesses risk falling under the CCPA by having a passive online presence.

The California Attorney General may fine companies up to $2,500 per non-willful violation and up to $7,500 per willful violation—amounts that add up quickly if a violation affects thousands (or millions) of users.

c. Other Relevant Consumer Data Protection Laws

Apart from California, 43 other states have made or are in the process of introducing forms of consumer data privacy bills. Wisconsin introduced three separate bills at the beginning of 2020 that would create rights and obligations concerning consumer data privacy similar to those created by the CCPA and the GDPR.

Currently, Maine and Nevada are the only two other states to have signed consumer data privacy protection bills into laws. The Maine privacy law applies only to internet service providers and not to independent businesses that may possess PII of users. The Nevada law is similar to CCPA in many ways, but it doesn’t apply to non-resident companies that do not actively do business in the state.

Additionally, in March 2020 Senator Jerry Moran (R-Kan.), introduced the *Consumer Data Privacy and Security Act*; however, the federal Congress has yet to take action on the proposed bill. If passed, this federal legislation would create a clear federal standard for consumer data protection and create specific rights of consumers to access, correct, and delete personal information. The proposed bill would also create substantial obligations for businesses, including those in Wisconsin, that use, collect, or otherwise possess PII. Finally, the proposed bill would provide the Federal Trade Commission (FTC) with the specific authority to enforce these rights and obligations.

In conclusion, while there are currently no Wisconsin or federal laws directly governing the regulation, storage, sharing, and use of personally identifiable information, Wisconsin businesses could be subject to the requirements of the CCPA or the GDPR. Additionally, it seems likely that in the near future, either Wisconsin or the federal government will pass a law that directly impacts Wisconsin businesses. Moving forward, it will be very important to understand how your company's collection of personal data may be impacted.

O'Neil, Cannon, Hollman, DeJong and Laing remains open and ready to help you.