A RECENT SUPREME COURT DECISION NARROWS THE SCOPE OF TRESPASSER IMMUNITY

A recent decision delivered by the Wisconsin Supreme Court has demonstrated that even a simple bar fight can have a drastic impact on Wisconsin's legal precedent. Such decision occurred in the case of *Stroede v. Society Insurance and Railroad Station, LLC*, where the court ruled that the off-duty employee who escorted a drunk patron out of a bar does not have immunity from the negligence lawsuit that followed when the patron fell down a flight of stairs and suffered injuries. *Stroede* sheds light upon the scope of immunity granted to "possessor[s] of real property" under Wis. Stat. § 895.529 against legal claims brought by injured trespassers.

The main facts of the case are as follows: David Stroede was drinking at a bar in Saukville, Wisconsin in 2014. Stroede became severely intoxicated and punched another bar patron. Initially, Stroede was removed from the bar by one of its on-duty employees. Jacob Tetting, an off-duty employee, was also in the bar that night having dinner with his family and witnessed Stroede attempt to re-enter the bar shortly after he was removed. Tetting grabbed Stroede by the shoulders and began to walk him out of the bar yet again. While escorting Stroede out, Tetting released Stroede near the bar's stairwell and Stroede tumbled down the stairs suffering serious injuries. Stroede, thereafter, filed suit against Tetting, the bar, and the bar's insurer.

Tetting argued that he was entitled to immunity under Wis. Stat. § 895.529, which states that "a lawful occupant of real property" has no duty of care to trespassers and because Mr. Stroede was a trespasser at the bar after he was initially removed for starting a fight, Tetting owed him no duty of care. However, the Court's decision hung on the determination of whether Tetting was an "other lawful occupant"[1] of the bar under the immunity statute. Ultimately, the Court found that because Tetting was simply a bar patron at the time Stroede was injured and he was not acting as an on-duty employee, he was not entitled to immunity.

Based on this ruling, off-duty employees are not entitled to immunity should they happen to injure a party trespassing at their place of employment. The application of *Stroede* is likely to be especially important in the future for employees of bars and restaurants. Thus, should a similar incident occur while you are enjoying a meal or a pint at your place of employment, let the on-duty employees handle the incident.

[1] Specifically, under Wis. Stat. § 895.529(1)-(2), an "owner, lessee, tenant, or other lawful occupant of real property" does not owe a duty of care to a trespasser of real property.

WISCONSIN LANDLORD SUBJECTED TO TENANCY IN JAIL

In a published opinion, the Wisconsin Court of Appeals confirmed that landlords who fail to provide timely statements explaining the basis for withholding funds from a residential tenant's security deposit may be subject to criminal prosecution and potential jail time.

In *State of Wisconsin v. Lasecki,* 2020 WI App 36, the Wisconsin Court of Appeals affirmed a circuit court judgment convicting Lasecki, a landlord, of two misdemeanor counts of engaging in unfair trade practices for failing to either return his tenants' security deposits in full or provide statements to the tenants explaining why he was authorized to withhold funds.

Generally, the Wisconsin Statutes allow a landlord to withhold from a tenant's security deposit amounts reasonably necessary to pay for certain authorized categories of costs or damages. A landlord that withholds such amounts from a security deposit is required to deliver to the tenant any remaining balance in the security deposit within 21 days.

Although the Wisconsin Statutes make no mention of any further requirement on the part of a landlord who elects to withhold amounts from a security deposit, the Wisconsin Administrative Code applicable to residential tenancies requires landlords that withhold any portion of a security deposit to deliver to the tenant a written statement accounting for all amounts withheld.

Lasecki's troubles began when his tenants filed a complaint with the Wisconsin Department of Agriculture, Trade and Consumer Protection (ATCP) alleging that Lasecki withheld their security deposits but failed to provide them with a statement accounting for the withholding. After Lasecki failed to cooperate with ATCP's investigation into the tenants' complaint, the local district attorney's office became involved, eventually charging Lasecki for his failure to comply with the provisions of the Wisconsin Statutes and Administrative Code pertaining to the return of tenant security deposits.

A jury eventually found Lasecki guilty of the criminal charges brought by the district attorney.

The circuit court thereafter awarded the tenants double their respective security deposits (as allowed by statute) and ordered Lasecki to a stayed sentence of 60 days in the county jail—14 days of which Lasecki served.

Lasecki appealed the jury verdict and order of the circuit court claiming that the circuit court lacked jurisdiction because the crimes of which Lasecki was convicted were "not known to law" and that no ordinary person would have sufficient notice that such conduct was criminal.

The Wisconsin Court of Appeals rejected Lasecki's arguments and instead affirmed his conviction, finding that the following framework within the Wisconsin Statutes and Administrative Code does provide notice that would enable an individual like Lasecki to know that his conduct was criminal in nature:

- Section 704.28 of the Wisconsin Statutes allows a landlord to withhold from a tenant's security deposit amounts reasonably necessary to pay for certain categories of authorized costs. This same section instructs landlords to deliver the full amount of any security deposit paid by tenant, less any authorized withholdings, within 21 days.
- While section 704.28 of the Wisconsin Statutes makes no mention of any requirement that a landlord provide a withholding statement to tenants, section ATCP 134.06(4)(a) of the Wisconsin Administrative Code provides that "[i]f any portion of a security deposit is withheld by a landlord, the landlord shall . . . deliver or mail to the tenant a written statement accounting for all amounts withheld."
- Section ATCP 134.01 of the Wisconsin Administration Code, entitled "Scope and Application," provides that chapter ATCP 134 "is adopted under authority of [Wis. Stat. §] 100.20.
- Accordingly, pursuant to section 100.26(3) of the Wisconsin Statutes, any person who intentionally refuses, neglects or fails to obey a regulation or order made or issued under section 100.20, shall, for each offense, be fined not more than $5,000 and imprisoned in the county jail for not more than one year.

After providing the above roadmap of how a landlord arrives at criminal liability for failing to provide a residential tenant with a security deposit withholding statement, the court of appeals' decision opines that an ordinary and reasonably prudent landlord would commonly consult with Chapter 704 of the Wisconsin Statutes (the landlord/tenant law chapter) and would also appreciate the need to understand landlord/tenant regulations set forth by the Wisconsin Administrative Code. The statutory and regulatory framework contained therein is, as the court put it, not beyond the comprehension of an ordinary landlord. As such, Lasecki had sufficient notice that his conduct could constitute a crime under Wisconsin law and the circuit court's verdict and order was affirmed.

The author of this article knows of no other instance in which a Wisconsin residential landlord has been criminally charged for failing to provide a security deposit withholding statement to a tenant. While most violations of this administrative code requirement are dealt with in civil proceedings, the court of appeals confirmed that such violations may also lead to criminal

charges. Here, charges may ultimately have been brought against Lasecki in response to his failure to cooperate with the state's investigation into the consumer complaint filed by his tenants; however, the court's decision should impress upon all residential landlords in Wisconsin the importance of providing tenants with a statement of all amounts withheld from their security deposit.

$7.5 MILLION DEBT LIMITATION FOR SMALL BUSINESS DEBTORS EXTENDED

On Saturday, President Biden signed into law the COVID-19 Bankruptcy Relief Extension Act of 2021. This act extends the $7.5 million debt limitation under the Small Business Reorganization Act of 2019 (SBRA) for another year, until March 27, 2022.

Last year, Congress passed the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) to provide emergency assistance for individuals and businesses affected by the COVID-19 pandemic. The CARES Act temporarily increased the debt limitation under the SBRA from $2,725,625 to $7.5 million. The SBRA, which took effect on February 19, 2020, created Subchapter V of the Bankruptcy Code to provide a more streamlined and cost-effective reorganization option for small businesses. The $7.5 million debt limitation increase under the CARES Act was set to expire on March 27, 2021.

The COVID-19 Bankruptcy Relief Extension Act of 2021 extends the bankruptcy relief provisions of the CARES Act, which most notably includes the $7.5 million debt limitation under the SBRA, until March 27, 2022. As a result, small businesses with debts between $2,725,625 and $7.5 million will continue to be eligible for Subchapter V for another year.

For further information regarding the COVID-19 Bankruptcy Relief Extension Act of 2021 or insolvency concerns relating to bankruptcy or receivership, please contact attorney Jessica K. Haskell.

FEMA LAUNCHES COVID-19 FUNERAL ASSISTANCE PROGRAM

Under the Coronavirus Response and Relief Supplemental Appropriations Act of 2021 and the

American Rescue Plan Act of 2021, the Federal Emergency Management Agency (FEMA) will provide financial assistance for COVID-19-related funeral expenses incurred after January 20, 2020.

FEMA estimates that qualifying families can expect reimbursements of $3,000 to $7,000 out of the program's total budget of $2 billion.

To be eligible for funeral assistance, you must meet the following conditions:

- The death must have occurred in the United States;
- The death certificate must indicate the death was attributed to COVID-19; and
- The applicant must be a U.S. citizen, non-citizen national, or qualified alien who incurred funeral expenses after January 20, 2020.

There is no requirement for the deceased person to have been a U.S. citizen, noncitizen national, or qualified alien.

FEMA will begin accepting applications for funeral assistance in April 2021. FEMA is still working out the details of this program, but encourages prospective applicants to start gathering the following documentation for the application:

- An official death certificate that attributes the death directly or indirectly to COVID-19 and shows that the death occurred in the United States;
- Funeral expense documents (receipts, funeral home contract, etc.) that include the applicant's name, the deceased person's name, the amount of funeral expenses, and the dates the funeral expenses happened; and
- Proof of funds received from other sources specifically for use toward funeral costs. FEMA will not duplicate benefits received from burial or funeral insurance, or financial assistance received from voluntary agencies, government agencies, or other sources.

If you have lost a loved one due to COVID-19 and have questions about the administration of your loved one's affairs, please contact Kelly M. Spott.

WANT TO CHALLENGE A WILL? HERE'S WHAT YOU SHOULD KNOW

If you are upset or disagree with the provisions of a will, you may be wondering if you should challenge it. In this article, we discuss a few grounds for challenging a will and what may happen if your challenge is successful.

A will may be challenged for several reasons. However, being upset or disagreeing with the provisions of a will is not enough. Instead, here are a few grounds for challenging a will:

- Lack of Formalities: The will wasn't executed pursuant to the formalities required under Wisconsin law. For example, the will was not signed by the testator (the person making the will) or witnessed by two non-relative and disinterested witnesses.
- Lack of Capacity: The testator lacked the requisite level of mental capacity to execute the will. For example, the testator suffered from dementia or a mental illness that prevented the testator from fully understanding his or her assets and the effect of the document.
- Undue Influence: The testator was unduly influenced by a relative, friend, care giver, or other third party to execute the will. Undue influence includes fraud, force, and coercion. To read more about undue influence, click here.

Upon a successful challenge, the will may be reformed or set aside completely depending on the circumstances.

Sometimes a will may contain a "no contest" provision that prescribes a penalty against an interested person for contesting the will. In these circumstances, a court may find that the no contest provision is unenforceable if the court determines that the interested person had probable cause for instituting the proceedings. *See* Wis. Stat. § 854.19.

The attorneys in the inheritance litigation team at O'Neil Cannon have extensive experience with will contests and other disputes relating to inheritance litigation. Because the rules for will contests are complex, we encourage you to reach out to the authors of this article or any other attorney in our inheritance litigation team with any questions or concerns you may have related to a will contest.

EUROPEAN DATA PRIVACY WATCHDOGS TAKE NEW STEPS

In the past week, European data protection authorities have found substantial European Union General Data Protection Regulation ("GDPR") violations and issued corresponding fines against high-profile companies. These decisions are informative for companies doing business in Europe as they indicate clear future enforcement priorities by European regulators.

On December 10, 2020, the French Data Protection Authority ("CNIL") issued fines against Google (€100M; $120M) and Amazon (€35M; ~$43M) for improper use of cookies on their websites. Specifically, the CNIL found that the tech giants automatically dropped tracking

cookies when users visited their French (.fr) websites. Under the GDPR, these tracking cookies cannot be used without prior consent by the user. Since at least October 2019, European law has been clear that websites must obtain prior consent before utilizing any non-essential cookies.

These fines follow a similar CNIL fine against Google for $57M for failing to adhere to the GDPR's transparency obligations.

Meanwhile, on December 15, 2020, Ireland's Data Protection Commission ("DPC") slapped Twitter with a fine of €450,000 (~$547,000) for failing to properly declare and document a data breach. The DPC is Europe's leading privacy enforcement agency for many large tech companies, including Facebook, WhatsApp, Google, Apple, and LinkedIn, among others. The DPC fine marked the first cross-border GDPR fine issued by the Irish watchdog. Though many have expressed concerns that the DPC has been slow in reacting to privacy violations by non-EU companies, this cross-border decision is somewhat of a landmark decision for the DPC. In addition to the Twitter case, the DPC has a backlog of over 20 cases against large tech firms, many of which are U.S.-based entities.

In 2020, both the CNIL and the DPC have recently issued guidance on cookie usage and the notice, consent, and transparency requirements of the GDPR. The Amazon and Google fines, together with the CNIL and DPC guiding opinions, provide insight into their enforcement priorities. The guiding opinions make it clear that the CNIL and the DPC are specifically targeting companies that are improperly utilizing non-essential cookies; furthermore, the extent of the fines indicate that the regulatory agencies view these matters as particularly egregious violations.

Moreover, the DPC's long-awaited first cross-border decision may be seen as a warning that non-EU companies may no longer find safe harbor in Ireland's lethargic enforcement efforts. Should these decisions act as a harbinger of future enforcement efforts, non-EU-based companies will need to quickly ensure compliance with GDPR regulations concerning non-essential cookies. As these decisions indicate, improper cookie usage could be costly for any company doing business in Europe.

If you or your company have questions or concerns about your cookie usage or compliance with international data privacy laws, please contact us.

FEDERAL TRADE COMMISSION AND

ENFORCEMENT OF PRIVACY LAW

As we have mentioned previously, there is no overarching federal data privacy law in the United States. By contrast, the European Union's General Data Protection Regulation (GDPR) regulates data privacy, including consumer data, in all sectors. Although there is no overarching federal data privacy law in the United States, there are a few sector-specific laws. In health care, for example, the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) govern many aspects of privacy. Also, the Telecommunications Act and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) touch on privacy issues in marketing. Still, there is no federal law specifically regulating the use of consumer data.

Despite the lack of consumer privacy statutes in the United States, the Federal Trade Commission (FTC) has been active for years in protecting American consumers against certain unfair and deceptive practices involving data privacy. The Federal Trade Commission Act (FTC Act) includes an extremely brief section that serves as perhaps the most important provision in U.S. privacy law. Section 5 of the FTC Act states simply: "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful." This single line, which does not specifically mention privacy, has been used by the FTC and Congress to make the FTC the de facto privacy enforcement agency of the federal government.

The FTC defines "Unfair Trade Practices" as any practice that results in a substantial injury, that lacks offsetting benefits, and cannot be easily avoided by consumers. In the privacy context, the FTC often looks at practices that unreasonably leave consumers' data vulnerable to hacking or theft. Should a company collect the personal data of an individual in connection with a product or services and make inadequate efforts to protect that data, the FTC may seek enforcement for violation of Section 5 of the FTC Act. Conversely, "Deceptive Trade Practices" involve material statements or omissions that are likely to mislead consumers who are otherwise acting reasonably. Deceptive practices can include false representations or false promises. Importantly, the FTC has taken the position that failure to adhere to the steps, standards, and promises contained in a privacy notice is a deceptive trade practice. Thus, for example, should a company state in its privacy notice that it will not transfer a consumer's data to a third party, any subsequent transfer of data to third parties is likely to be considered a deceptive trade practice.

The financial penalties for unfair or deceptive trade practices can be enormous. These financial penalties can be imposed through a consent decree or through fines imposed by the FTC and approved by the courts. In many instances, the FTC will seek a consent decree with the company through which the company agrees, without admitting guilt, to pay certain fines, stop the alleged practices, or implement new or improved privacy policies and practices. Alternatively, if the company refuses to enter a consent decree, the FTC can seek

judgment through an administrative law judge. Should the company refuse to adhere to the FTC ruling, it may be fined up to $43,280 per violation and be liable for any damages caused by the alleged acts. Importantly, each instance of the alleged privacy violation constitutes a unique violation for the purposes of such penalties, leading to potentially substantial fines.

Over the past several years, the FTC has been increasingly active in enforcing unfair and deceptive trade practices that concern consumer data privacy. In 2019 alone, the FTC brought 130 spyware and spam cases as well as 80 general privacy lawsuits. The biggest privacy case of 2019 was *In the Matter of Facebook*, in which the FTC and the social media giant agreed to a consent decree requiring Facebook to pay a five billion dollar fine and institute a broad and privacy-related corporate restructuring. This year, the FTC has commenced 102 actions related to privacy, including cases against Zoom Video Communications, Inc., Williams Sonoma, Inc., and the Western Union Company.

The ability of the FTC to impose substantial penalties on companies who willingly or unwillingly deviate from the practices described in their privacy notices makes it extremely important to routinely review and update your company's privacy notice to ensure that it accurately depicts your company's privacy practices.

IS YOUR HOTEL WEBSITE IN COMPLIANCE WITH THE ADA?

There has been a trend recently in the state of Wisconsin, and elsewhere, for attorneys to file lawsuits against hotel owners alleging that their websites are in violation of the Americans with Disabilities Act ("ADA") because they are not accessible to disabled individuals. Specifically, the complaints allege that the hotel websites are in violation of the ADA because they fail to identify accessibility features, do not allow for booking of accessible rooms, and do not provide sufficient information regarding accessible rooms and amenities at the hotel.

Frequently, the attorneys bringing the lawsuits against the hotel owners will represent the same disabled party (often referred to as a "tester"), use a stock, form set of allegations against several hotel owners, and file more than one lawsuit at a time. Based on the sheer volume of these cases in recent weeks, it is unlikely these lawsuits will cease any time soon.

The parties filing the lawsuits typically assert that hotel owners must ensure that their website (and the third-party booking websites used to reserve their rooms) meet certain requirements. For example, the plaintiffs assert that hotel websites must:

- identify and describe accessible features in the hotels and guest rooms offered through their reservation service in enough detail to reasonably permit individuals with disabilities to assess independently whether a given hotel or guest room meets their accessibility needs;
- ensure that assessible guest rooms are held for use by individuals with disabilities until all other guest rooms of that type have been rented and the accessible room requested is the only remaining room of that type; and
- reserve, upon request, accessible guest rooms or specific types of guest rooms and ensure that the guest rooms requested are blocked and removed from all reservations systems.

If you or your business receives a demand letter threatening legal action or are served with a lawsuit, you should promptly contact an attorney to discuss your options.

WISCONSIN BUSINESSES AND COMPLYING WITH CONSUMER DATA PROTECTION LAWS

As we have previously covered, Wisconsin businesses may be subject to the requirements of the European Union General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). Additionally, many states, including Wisconsin, and the federal government are considering similar data protection bills that may impact Wisconsin businesses. With overlapping obligations, compliance with data protection laws is an increasingly tricky business for most companies. To ensure that your company doesn't inadvertently violate any current or future laws, consider the following six steps:

Step 1: Consider the Applicability of Data Privacy Laws

Companies should determine whether existing consumer data privacy laws apply to them. The GDPR applies to companies (1) established in the EU and conducting data processing in the context of that business's activities; or (2) either: (a) offering goods or services, for free or for a fee, to individuals in the EU or (b) monitoring the behavior of individuals within the EU.

Wisconsin companies with a physical presence in the EU will almost certainly be subject to the GDPR. Without a physical presence, a Wisconsin company will nonetheless likely fall within the GDPR's scope if it offers products or services to EU individuals or businesses or if it monitors the online behavior of EU individuals or businesses.

On the other hand, the CCPA will apply to your business if it is a **for-profit business that does business in the state of California and collects** California consumers' personal

information (or such information is collected on its behalf) and determines the **purposes and means** of processing California consumers' personal information, AND if it meets *one* of the following criteria:

- It has at least **$25 million** in annual gross revenues;
- It buys, sells, shares, or receives the personal information of at least **50,000 California consumers, households, or devices** per year; *or*
- It derives at least **50 percent** of its annual revenue **from selling** California consumers' personal information.

Most companies should be able to determine whether they meet the above criteria. Some businesses may struggle to determine whether or not they buy, sell, share, or receive the personal information of at least **50,000 California consumers, households, or devices** per year. Still, companies with even a small or moderate online presence will likely meet this threshold due to the broad scope of the CCPA's definition of personally identifiable information (PII).

Once you have determined that the GDPR or CCPA applies, take affirmative steps to ensure that you are in compliance.

Step 2: Map Your Company's Data

Once you have determined that the GDPR or the CCPA applies to your company, you must map the data that your company collects. Mapping will include knowing the type of data you are collecting, its source, and what happens to the data after it has been collected. You should also identify where the data is kept, what encryption or other security your company uses to protect that data, who has access to the data, and whether there are any security risks.

This step is necessary and must be taken to understand what data your company collects and where and how it is stored so that you can take appropriate steps to ensure efficient compliance with applicable data protection rules.

Step 3: Clean Up Your Company's Data

Companies should be disciplined and strict about data collection. Determine what information is necessary and what information is superfluous. Moreover, think about why certain PII is retained, rather than deleted, in view of the company's data collection goals. You may find a greater financial gain in deleting troves of PII as opposed to investing in storage and encryption. Moreover, deleting unnecessary files can help reduce the risk of inadvertently committing data protection violations.

This step will not only help ensure compliance, but it will also allow you to develop an

effective and potentially financially valuable strategy for data collection.

Step 4: Create Privacy Protection Procedures and Policy

To ensure that consumers may exercise the rights to their PII granted to them under the GDPR and the CCPA, your company must have efficient processes. In crafting a privacy protection policy, consider:

- how individuals can give consent for data collection and transfer;
- the process for a consumer to request data deletion or to opt-out of data collection;
- how the company can ensure complete, effective data deletion or tagging across all platforms;
- the process for responding to a hypothetical data breach; and
- how the company can ensure that minors give proper consent.

When creating privacy procedures and policies for your company, it is important to understand that the relevant consumer data privacy laws require transparency in matters concerning PII. Therefore, your company's privacy procedures and policies must be drafted carefully and with the complex obligations of the GDPR or the CCPA in mind.

Step 5: Update Your Company's Online Privacy Policy

Under the GDPR or the CCPA, your company must have an easily accessible and understandable privacy policy. To ensure that your company's privacy policies comply with the GDPR and the CCPA, you must ensure that it contains the following:

- A statement to residents of California or the EU that they have the right to opt-out of the sale of their data;
- An explanation that indicates how the company will inform consumers of future privacy policy updates; and
- A description of how the consumer's data will be used, including all possible uses that involve a transfer of that data.

Furthermore, you must update your company's privacy policy at least once every 12 months and notify consumers of each such update. As discussed, every privacy policy must be easily accessible and transparent. Even unintentionally complex policies may expose your company to liability.

Step 6: Update Your Company's Website

Finally, to comply with the GDPR and the CCPA, a company must include a link on its website that says "Do Not Sell My Personal Information." The link must use that specific phrasing and bring users to a page that allows them to opt-out of any sale of their data. This link must be separate from the general privacy agreement and cannot require the consumer to create a

profile or account to access the opt-out. The CCPA also requires companies to create a toll-free number for consumers wanting to opt-out of the sale of their data.

After a consumer opts out, a company has two options under the CCPA: (1) it can retain the consumer's PII but exclude that PII from any sale, or (2) it can delete the consumer's data entirely. However, the GDPR requires the company to delete the consumer's data entirely. Thus, it is very important to understand whether the CCPA or GDPR (or both) applies and to have specific procedures in place to respond to a consumer's request to opt out.

What to Expect in Wisconsin

Because the GDPR and the CCPA are intentionally extraterritorial, their obligations may easily reach Wisconsin businesses. Furthermore, because of the steep fines for violating these data protection laws, Wisconsin businesses must either confirm that they are not subject to these strict requirements or take proactive steps to ensure compliance.

Even if the GDPR and the CCPA currently do not apply to your company, it may not be long until Wisconsin or the federal government implements a consumer data protection law that does. Consequently, regardless of whether you do business in the European Union or in California, beginning to implement better data collection practices now may help your companies online reputation and reduce future risks.

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

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.