LATIMER LEVAY FYOCK

# ONLINE DANGER:
# PROTECTING YOUR BUSINESS FROM CONSUMER CLASS ACTIONS AND OTHER RISKS ASSOCIATED WITH OPERATING A WEBSITE

With everyone everywhere doing everything online, businesses know the value of their websites are more important than ever. Companies have a lot to think about when it comes to setting up or revamping a website including the ultimate purpose, level of interactivity and the amount of data collected. It is vital that companies also address critical legal issues associated with the operation of a website. The failure to do so can leave businesses exposed to serious risks, including the possibility of costly and disruptive consumer class action lawsuits. Identifying and addressing these issues can minimize the legal, financial, and reputational risk. For example, here are a few important issues to consider.

## 1. Terms of Service

Businesses which provide access to its services or products online must have well-defined Terms of Service ("TOS"). In a TOS, a business can provide important disclaimers, limitations on liability, warnings to consumers, arbitration provisions and other liability reducing provisions. Given there are certain disclaimers and warranties which are commonly used, there can be a temptation for businesses to simply "cut and paste" a TOS from another's website. However, this is a dangerous short-cut as a copied TOS may not be appropriate for the business and the business could be liable for copyright infringement. To really be protected and minimize risk, business representatives need sit down with a competent lawyer to tailor the TOS to the needs of that business.

Just as important as drafting a TOS which is specific to that business is the method in which the TOS will be presented to the public. In what should not be a surprise to anyone, the law is still catching up to the rapid progression of technology. While online agreements are relatively new to judicial analysis, the basic requirements for any agreement also apply to online agreements.

For a TOS to be enforceable, the user of the website must have outwardly expressed, either through words or conduct, his or her assent to the TOS. Under Illinois contract law, a website must provide a user with reasonable notice that his or her use of the website or click on a button constitutes assent to an agreement. To comply with the notice requirement three methods have been adopted by businesses:

- The "browsewrap agreement" attempts to bind a user of a website to the TOS simply by the user's act of browsing the website, without ever requiring the user to affirmatively do something, like check a box, to indicate his or her assent to the TOS. Courts have generally found that TOS presented as a "browsewrap" are not enforceable because they do not allow for enough outward expression of assent by the user.
- A "clickwrap agreement" is formed when website users click a button or check a box that explicitly affirms that the user has accepted the TOS after having the opportunity to scroll through the terms posted on the website. This type of agreement is generally enforced.
- The "sign-in-wrap agreement" is the third type of online contract. With this type of online agreement, users do not need to take an affirmative action to explicitly agree to the TOS (such as clicking a box explicitly affirming that the user accepts the terms after having the opportunity to scroll through them), but it does require some form of affirmative action by requiring the user to sign up for an account. Sign-in-wraps are regularly upheld where a hyperlink to the TOS appears next to the only button that will allow the user to continue use of the website.

Over the last few years, judges in both federal and state courts have begun to evaluate the different ways of presenting TOS online to determine whether the method of presentation supports a finding that the user assented to the TOS, i.e., that they are enforceable. As the law continues to evolve and catch up with technology, it will be important to regularly evaluate and update both the content of the TOS and how they are presented. Having the proper TOS and presenting them in the right way could be the difference between getting trapped into years of costly litigation and avoiding litigation altogether.

## 2. Compliance with the Americans with Disabilities Act

The Americans with Disabilities Act ("ADA") requires certain businesses to make accommodations for people with disabilities to enable them to access the businesses' services, goods, or information to generally the same degree as any non-disabled individual. The ADA was passed before the mainstreaming of internet-based business content, resulting in no clear guidance as to whether online platforms are subject to the same accessibility requirements as physical locations. However, some courts have treated web content as no different than a bricks-and-mortar storefront, holding that a business's electronic presence (website, mobile services, internet commerce, etc.) should be as accessible to hearing- and visually-impaired users, and those who must navigate by voice, screen readers or other assistive technology, as non-disabled individuals. While there is also case law in the other direction, fighting a lawsuit about the applicability of the ADA is likely a more

expensive prospect than simply complying.

Businesses that fall under the category of "public accommodation" are covered by Title III of the ADA. In addition, businesses that have at least 15 or more employees are covered by Title I of the ADA. Businesses that fall under either Title I or Title III should aim to ensure that their websites and any other online or e-platforms offer "reasonable accessibility" to people with disabilities. Businesses who are subject to Title I of the ADA should ensure that all of their electronic systems and communications are accessible to any disabled employee – including any intranet, networks, and internal messaging (voice, chat, email). Failing to create an ADA-compliant website could expose a business to lawsuits, financial liabilities, and damage to brand reputation. Lawsuits against businesses regarding ADA violations have exploded recently and in Illinois number of ADA lawsuits rose a staggering 170% from 2019 to 2020.[1]

Given the rise in lawsuits, businesses should work with their attorneys to make sure their websites are compliant with ADA guidelines.

### 3. Compliance with Data Privacy and Protection Laws

When a business owns and maintains a website it collects large amounts of personally identifiable information from visitors and users of the website. This collection of information means businesses need to comply with data collection and privacy laws. Illinois has one of the most stringent data breach laws in the country. The Illinois Personal Information Protection Act ("PIPA") imposes strict requirements on public or private entities that handle, collect, disseminate, or otherwise deal with nonpublic personal information. Nonpublic personal information includes either (a) a username or email address along with its accompanying password or other method to access an online account, or (b) a person's first name or first initial and last name along with a social security number, driver's license number, state identification card number, account number, credit or debit card number, medical information, health insurance information, or biometric data.

The PIPA requires businesses that collect data to implement and maintain reasonable security measures to protect users' personal information from unauthorized access, acquisition, destruction, use, modification or disclosure. Further, the PIPA requires that personal information be disposed in a manner that renders it "unreadable, unusable, and undecipherable." Failure to dispose of personal information in compliance with the PIPA is subject to a civil penalty of up to $100 for each violation. In addition, the Attorney General has the authority to bring an action to remedy a violation of the PIPA's disposal requirements.

[1] See, https://www.prometsource.com/blog/illinois-increase-ada-lawsuits accessed February 19, 2021.

The PIPA also imposes specific steps that must be taken if a data breach occurs. For example, a company that owns or licenses personal information must notify Illinois residents of a breach in the most expedient time possible and without unreasonable delay. The disclosure must include the toll-free numbers, addresses, and websites of consumer reporting agencies and the Federal Trade Commission. The disclosure most also state that the individual can obtain information from these sources about fraud alerts and security freezes.

Significantly, the PIPA expressly provides that a violation of the Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Businesses Practices Act. Because a violation of the PIPA is a per se violation of the Consumer Fraud Act, a failure to comply with it exposes a business to expensive and damaging class action litigation.

While the PIPA is a strong law, California recently enacted a Consumer Privacy Act ("CCPA") which goes beyond PIPA. Given that California is on the forefront of privacy law it should be expected that Illinois and other states will in due course adopt the language of the CCPA. Thus, businesses should consider adopting the California standard in order to avoid future liability. The CCPA imposes several affirmative requirements for website operators, including:

- **Initial Notice:** if a website collects user information, it must inform the user of the categories of personal information collected and the purposes of the use;
- **Website Notice:** businesses must disclose on their website the rights consumers are allowed to exercise under the CCPA, including the right to: (a) know about the personal information collected about them and how it is used and shared, (b) have certain information deleted, (c) demand that personal information not be sold to third parties, and (d) not to be punished by the website operator as a result of exercising these rights; and,
- **Optout Notice:** if the website sells consumer information, it must provide a "clear and conspicuous" link on the homepage that says, "Do Not Sell My Personal Information."

Only California residents have rights under the CCPA. However, a California resident has the right to sue a business if his or her nonencrypted and nonredacted personal information was stolen in a data breach because of the business's failure to maintain reasonable security procedures and practices to protect it. In fact, there has been a growing number of lawsuits brought under the CCPA, including cases brought against companies such as Zoom, Marriott, Facebook, LinkedIn, TikTok, Instagram and Walmart. Because websites reach across state lines, every business operating a website should be aware of and compliant with other state's privacy laws, including the CCPA.

## 4. Compliance with the Illinois Biometric Information Privacy Act

In addition to the PIPA, Illinois has enacted a law that specifically addresses the collection, retention and destruction of biometric data. With the increase in use of voice recognition software and facial, retina and fingerprint scanners, concerns over how companies are storing, using and destroying biometric information is also growing. In 2008, Illinois published the first biometric privacy law in the United States, known as the Biometric Information Privacy Act ("BIPA").

Over the past few years, there has been an explosion of class action lawsuits brought under the BIPA. One notable case that should serve as a warning to any business collecting biometric information is the class action lawsuit brought against Facebook, which recently settled for $650 million.

The BIPA imposes five obligations on private companies (excluding some businesses, such as certain financial institutions) who collect, use or share biometric information, like voiceprint, retina scans, fingerprint scans, and facial scans.

1. **Written retention and destruction policy:** Private entities must develop and maintain a written policy that is made available to the public establishing a retention schedule and guidelines for permanently destroying biometric data.
2. **Written release:** Private entities are prohibited from obtaining biometric data without informed written consent.
3. **Prohibition against profiting:** Private entities cannot sell, lease, trade or otherwise profit from biometric data.
4. **Restrictions on disclosure:** With limited exceptions, private entities cannot disclose or otherwise disseminate biometric data.
5. **Security requirements:** Private entities in possession of biometric data must use reasonable standards of care applicable to that entity's industry to protect the biometric data.

A violation of the BIPA carries significant consequences. The statute imposes damages of at least $1,000 per violation for negligent violations. Intentional or reckless violations will cost at least $5,000 per violation. In addition, the statute provides for an award of reasonable attorney's fees. Significantly, a consumer does not need to prove that he or she suffered an actual injury from a violation of the BIPA to recover. The Illinois Supreme Court has held that a procedural violation of the BIPA on its own is sufficient to support a private right of action.

That decision by the Illinois Supreme Court is having far-reaching consequences. A common strategy in defending class action litigation is to remove the lawsuit to federal court under the Class Action Fairness Act. However, for federal courts to have jurisdiction pursuant to Article III of the U.S. Constitution, the plaintiffs must have alleged an "injury in fact." In *Thornley v. Clearview*, Inc., the Seventh Circuit Court of Appeals recently held that where the plaintiffs have alleged a "bare procedural violation" of the BIPA, "divorced from any concrete harm," the complaint fails to give rise to federal court jurisdiction under Article III. Thus, by alleging a bare procedural violation with no actual injury, the plaintiffs succeeded in alleging claims that can be resolved only in Illinois state court.

Furthermore, the law on other common defenses to BIPA claims, such as preemption by federal labor laws and statute of limitations, is still unsettled, with two cases pending in an Illinois appellate court on the applicable statute of limitations and one case pending in the Illinois Supreme Court on the issue of preemption.

The best and most inexpensive defense to a BIPA case is simple: avoid litigation altogether by hiring competent counsel to walk you through the statute and assist you in making sure that all steps are being taken to ensure compliance with the BIPA's requirements. As Facebook and many other companies have learned, failure to comply with the BIPA can be a costly mistake. Fortunately, however, with the right counsel, it is a mistake that can be avoided.

## LET US HELP

Whether you are a business who has already found itself on the wrong end of a lawsuit, or you need help ensuring that your business' website complies with applicable laws and mitigates risk to avoid litigation, we welcome the opportunity to help. Please contact **Robert Carroll** at **rcarroll@llflegal.com** or **Brian D. LeVay** at **blevay@llflegal.com** if you have any questions or comments.