WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Wrapping Your Privacy Practices Up with a Bow

Written By **Angela P. Doughty, CIPP-US** (apd@wardandsmith.com)
December 19, 2017

For many companies, the "hap-happiest season of all" coincides with the busiest season of all. Business owners and employees are racing to fill customer orders in time for the holidays, which also means an avalanche of new personal information that must be protected, including customer names, shipping addresses, email addresses, and credit card numbers. To avoid the privacy and data security holiday blues, and instead enjoy the hustle and bustle of this holiday season, consider these data privacy and security tips:

Don't hang your stocking on public information

The definition of "personal information" varies by law and by state, but it usually includes some combination of a person's name, address, phone number, and other information that could reasonably be used to identify the person.

Often, this personal information is freely available through a quick Google search, or on easily accessible online directories or databases. The public nature of certain personal information leads many companies to incorrectly believe that they can escape their responsibilities related to data privacy and security, because the information they have collected is already "out there" or not "highly sensitive." However, this is not necessarily the case. Not all states have a "public" exception in their data breach notification laws, and certain industry-specific laws do not distinguish between freely accessible personal information and personal information that is "private." Whether data privacy and security laws apply to certain "public" information will often depend on the information and how and when it was collected.

Encryption is the gift that keeps on giving

When a company becomes the victim of a security breach (such as hacking, phishing, or ransomware attacks), nearly all state laws require the company to notify every single individual whose personal information was compromised of the breach. Notification laws vary by state, and the company must follow the notification law of the state in which the individual resides (not the one in which the company is located).

This is a time-consuming and expensive process, but the good news is that it can potentially be avoided. The vast majority of states have exceptions to their notification requirements, meaning that if your company has encrypted all of its information to make it unreadable, and the encryption key has not been compromised, notification may not be required.

Certain states require that specific encryption methods be used in order to trigger application of a notification

exception, so consider selecting an encryption method that complies with Federal Information Processing Standard Publications ("FIPS"), which are computer system standards developed by the federal government.

Like a holiday fruitcake, sometimes your data can stick around too long

One overarching principle of good privacy and security protocol is to retain personal information only as long as needed for the purpose in which it was collected. Consider reviewing the length of time your company retains personal information and analyze the purpose for which it is collected. If certain information is no longer needed, securely delete or destroy it.

Your data management process may be affected by a particular federal, state, or industry-specific law on data destruction and retention requirements, so be sure to understand all of the applicable state and federal laws to the personal information collected, stored, and destroyed.

A misleading or non-existent privacy notice can put you on the FTC's naughty list

If your company maintains a website, you should have a privacy notice, often called a "privacy policy," clearly posted on the website. The privacy notice should, at a minimum, inform website users and customers about the type of information your company collects and how that information is collected, stored, used, and shared.

Certain states also require specific provisions to be included in privacy notices (California's law is the most stringent). These state requirements may be applicable to your company's privacy notice even if your company is not located in that particulate state, such as when your company does business in that state or collects information from residents of that state. Additionally, some industry-specific laws have other requirements related to the content and communication of privacy notices.

While it may be tempting for your company to promise customers that their personal information is 100% safe, the Federal Trade Commission can bring enforcement actions for deceptive trade practices against a company for violating its own privacy policies, so be sure to not only have a privacy policy, but one that accurately reflects the data privacy and security practices of your company.

The United States has a holiday buffet of privacy laws

Unlike Europe, the United States does not have a singular set of overarching data privacy and protection regulations. Instead, the United States has a patchwork of federal, industry-specific laws, which work in concert with state laws that vary widely in content and application. North Carolina, for example, has a statute governing the destruction of personal information (N.C. Gen. Stat. 75-64); one of the nation's strictest data breach laws which requires reporting to the Attorney General, the provision of credit monitoring (N.C. Gen. Stat. 75-65); a specific statute on how to collect, store, and send Social Security Numbers (N.C. Gen. Stat 75-62); and a statute governing interception of wire, oral and electronic communications (N.C. Gen. Stat. 15A-287). It is critical that all companies understand which privacy and data security regulations apply to the information collected and stored within its systems.

Conclusion

While no system is Scrooge-proof, the implementation of proper cybersecurity policies and procedures, as well as awareness of the regulations that affect your data, can help ensure a successful holiday season and a prosperous New Year for your business.

--

Angela P. Doughty, CIPP-US.

This article is not intended to give, and should not be relied upon for, legal advice in any particular circumstance or fact situation. No action should be taken in reliance upon the information contained in this article without obtaining the advice of an attorney.

We are your established legal network with offices in Asheville, Greenville, New Bern, Raleigh, and Wilmington, NC.