ARTICLE FOR CLE CREDIT

Privacy Rights and Data Breaches

BY BRIAN J. PEZZILLO, ESQ.

Consumers face a variety of threats that continue to grow on a daily basis. One of the most pervasive is the loss of personal, private information, often referred to as Personally Identifiable Information (PII).

The issues of privacy, privacy rights and data breaches are in the headlines nearly every day as a debate is currently ongoing regarding how to define privacy and what rights associated with privacy should be protected. While there appears to be a general acceptance that consumers' privacy is deserving of protection, there is not a consensus as to what specific rights should be granted to consumers, nor the best way of protecting those rights. To date, there have been a number of different approaches with regard to protection of privacy rights. Widely considered to be the gold standard of data protection is the European Union's General Data Protection Regulation (GDPR), which was enacted in 2016 and took effect May 25, 2018. The GDPR is based on the principle that privacy is a fundamental human right. *See* GDPR, Art. 1(2). One of the key principles of the GDPR is that data belongs to the "data subject," or individual, and that the data cannot be used without the data subject's consent (GDPR Art. 7) and must be done so in a lawful, fair and transparent manner. *See* GDPR, Art. 83(5). The GDPR applies to data held by not only private companies or individuals but also to governmental actors as well. GDPR Art. 2, 4(7, 8). Underscoring the treatment of privacy rights in Europe, the GDPR allows for fines as high as 4 percent of global revenue for those who infringe on certain rights.

While many other countries have chosen to adopt privacy regulations similar to the GDPR, the U.S. has not yet enacted an omnibus, comprehensive federal privacy framework. While such a framework is likely inevitable, the timing and specifics of what will be included in such legislation is not known. This has left the U.S. with a patchwork of numerous federal and state laws that address different industries and different state consumers in a variety of fashions. Examples of various federal laws include the Gramm Leach Bliley Act (GLBA) (addressing non-public information held by financial institutions), Health Information

Portability and Accountability Act (HIPAA) (protects information concerning health status, provision of health care or payment for health care that can be linked to an individual), Federal Trade Commission Act (addressing unfair and/or deceptive trade practices), the Children's Online Privacy Protection Act (COPPA) (restricting the gathering of information from children online) and many more.

When one looks to individual states, most states have not enacted comprehensive privacy protections. A notable exception to this rule is California. In June 2018, the California Legislature enacted the California Consumer Privacy Act of 2018 (CCPA). The provisions of the CCPA became effective January 1, 2020. The CCPA protects individual residents of California. The CCPA applies only to businesses. One qualifies as a business if one of three criteria are met:

1) Annual gross revenue in excess of $25 million;
2) Annually buy, receive for commercial purposes, sell or share for commercial purposes, the personal information of 50,000 or more consumers, households or devices; or,
3) Derive 50 percent or more of your annual revenue from selling consumer's personal information. *See* Section 1798.140(6)(1)(A-C).

If one of the preceding criteria are true and all the following criteria are true, then you are considered a business subject to the provisions of the CCPA:

1) You are a sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organized or operated for the profit or financial benefit of your shareholders or other owners;
2) You collect consumers' personal information, or someone collects it on your behalf;
3) You alone, or jointly with others, determine the purposes and means of the processing of consumers' personal information; and,
4) You do business in California.

"Doing business" is not defined by the CCPA; however, based upon the wording of the statutes it is well accepted that the CCPA has extra-territorial reach and is not limited to just those businesses that are physically located in California. This understanding has wide-ranging implications, as many businesses do business in California, including many located in Nevada.

The CCPA provides consumers new rights, including the right to request:

1) The categories of personal information the business has collected about the consumer;
2) The categories of sources from which the personal information is collected;
3) The business or commercial purpose of collecting or selling personal information;
4) The categories of third parties with whom the business shares personal information; and,
5) The specific pieces of personal information the business has collected about the consumer. *See* Section 1798.110.

Likewise, consumers must be advised of their rights pursuant to Section 1798.115 to request:

1) The categories of personal information that the business collected about the consumer;
2) The categories of personal information that the business sold about the consumer;
3) The categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold; and,
4) The categories of personal information about the consumer that the business disclosed for a business purpose.

In keeping with the modern trend of empowering and allowing consumers to control how their information is used and transferred, the CCPA grants to consumers the right to request erasure of "any personal information about the consumer which the business has collected from the consumer." *See* Section 1798.105. This right likely finds its genesis in Europe's GDPR, which provides for the same right. Likewise, consumers may opt out of having their personal information sold. *See* Section 1798.120(a-c). To meet their obligations regarding the opt-out right, businesses must provide a "reasonably accessible" and "clear and conspicuous link" on their homepage titled "Do Not Sell My Personal Information."

Nevada has also enacted statutes for the protection of consumers. Nevada's protection is primarily designed to address online activities and controls the activities of "operators," which is defined as one who:

a) Owns or operates an internet website or online service for commercial purposes;
b) Collects and maintains covered information from consumers who reside in this state and use or visit the internet website or online service; and
c) Purposefully directs its activities toward the state of Nevada, consummates some transaction with the state of Nevada or a resident thereof, purposefully avails itself of the privilege of conducting activities in this state or otherwise engages in any activity that constitutes sufficient nexus with Nevada to satisfy the requirements of the U.S. Constitution.

"Covered information" is defined as:

1) A first and last name;
2) A home or other physical address that includes the name of a street and the name of a city or town;
3) An electronic mail address;
4) A telephone number;
5) A Social Security number;
6) An identifier that allows a specific person to be contacted either physically or online; and,
7) Any other information concerning a person collected from the person through the internet website or online service of the operator and maintained by the operator in

CONTINUED ON PAGE 16

CONTINUED FROM PAGE 15

Privacy Rights and Data Breaches

combination with an identifier in a form that makes the information personally identifiable.

Nevada's privacy notice requirement is found in NRS 603A.340(1) and requires that the notice identify the categories of covered information that the operator collects through its internet website or online service and the categories of third parties with whom the operator may share such covered information, a description of the process, if any such process exists, for an individual consumer who uses or visits the internet website or online service to review and request changes to any of his or her covered information that is collected through the internet website or online service, describes the process by which the operator notifies consumers who use or visit the internet website or online service of material changes to the notice required to be made available by this subsection; discloses whether a third party may collect covered information about an individual consumer's online activities over time and across different internet websites or online services when the consumer uses the internet website or online service of the operator; and states the effective date of the notice. Unlike data subjects under the GDPR, Nevada does not provide for a private right of action. Instead, the Nevada Attorney General has the right to enforce the provisions of the law and in the event of an alleged violation may seek both injunctive relief as well as civil penalties in the amount of $5,000 per violation.

Data privacy is a complex and rapidly evolving area of law, and it must be tracked on a daily basis as change is a constant. It should be expected that new and comprehensive laws are forthcoming. In the meantime, it is imperative that all businesses conduct business in an open and transparent fashion and honor commitments to treat consumers' data as personal rights to be protected accordingly.

BRIAN J. PEZZILLO is a member of Howard & Howard Attorneys, PLLC, where he practices in the areas of construction law, privacy and cybersecurity, administrative law, public works and contracting, commercial and business law, contract negotiation, alternative dispute resolution, litigation and appeals. Pezzillo earned his B.B.A. degree from the University of New Mexico, Albuquerque, and his J.D. degree from the University of New Mexico School of Law in Albuquerque, New Mexico, and a graduate certificate from Drexel University in privacy and cybersecurity.