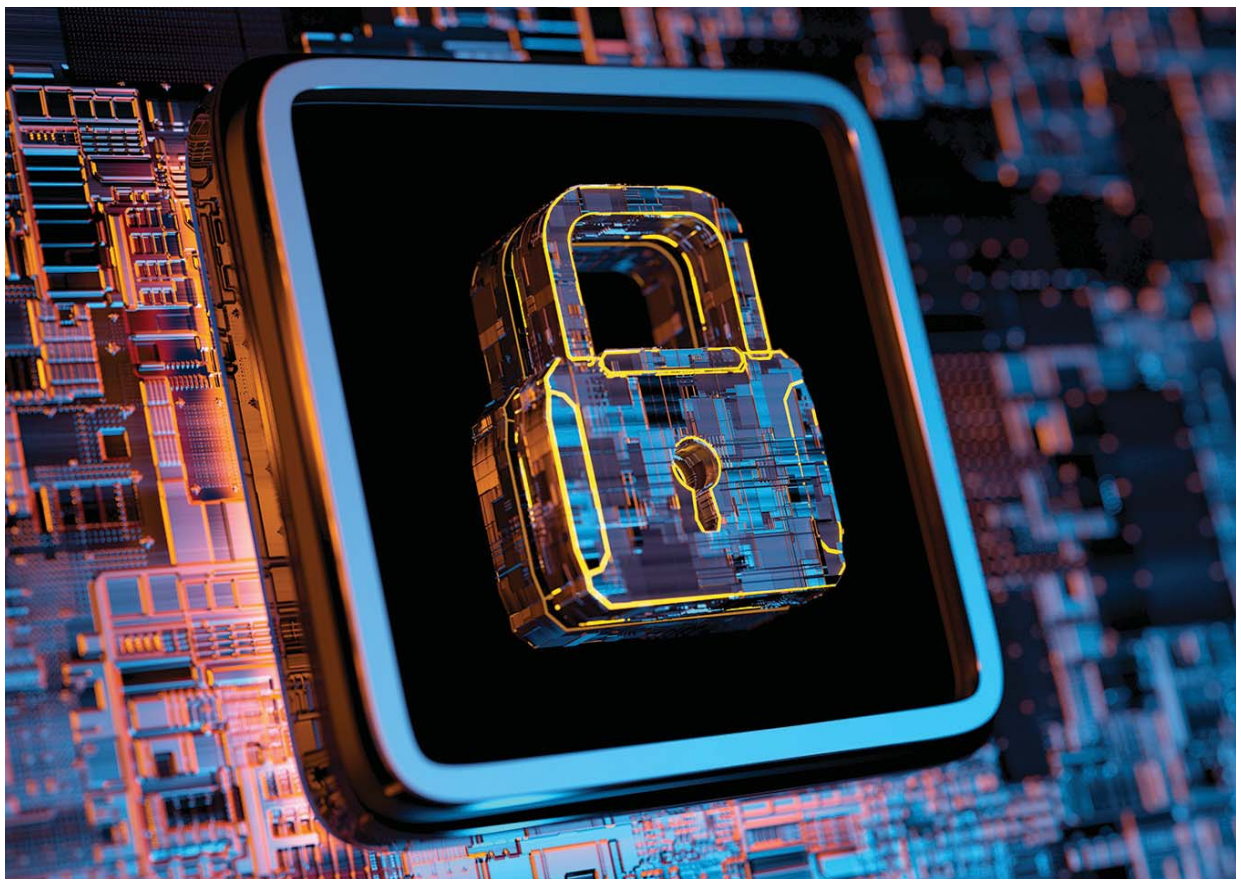
SPOTLIGHT ON

Data Privacy, Retail & Consumer Goods

Your Computers & Privacy: Ready or Not, There They Go

By DAVID LAM



Our right to privacy is being challenged in new and urgent ways. As consumers, we must be aware of the impact our choices have on privacy. As businesses, we must know our obligations to protect Personally Identifiable Information (PII) we collect from customers, employees, and others. This obligation has taken on increased urgency as cybercrime has grown to epidemic levels and it is too easy to access, steal, change, and destroy information.

Concerned with these privacy challenges, in 1995 the European Union led the world in electronic privacy by adopting the European Data Protection Directive. This was replaced in 2018 with the General Data Protection Regulation (GDPR) – which as many of us know, applies to any organization that collects the PII of Europeans.

In 2018 the California legislature passed the California Consumer Privacy Act (CCPA) which went into effect on January 1, 2020. Then, in a bid to strengthen the law, privacy advocates received a major victory when the California Privacy Rights Act (CPRA) was passed in November 2020. Aside from a few provisions, the CPRA goes into effect in 2023.

The CCPA established the requirement for businesses to provide consumers certain notices explaining their privacy practices and gave consumers more control over the personal information that businesses collect about them, including the rights to (among others):

- Know what PII a business collects, how it is used and shared;
- Delete the PII collected from them; and
- Opt-out of the sale of their PII.

For-profit businesses are covered by the CCPA if they meet any of the following:

- Greater than $25 million in annual revenue,
- Buy, sell or receive over 50,000 personal records,
- Receive at least 50% of their annual revenue from selling personal information.

The new CPRA, however, changes the record threshold to 100,000 records and now includes revenue generated from sharing personal information. The CPRA also adds the new category of sensitive personal information.

Included in these laws are the right to have information protected at a commercially reasonable level. Without such protection, both California privacy laws provide for penalties and an ability for individuals to receive compensation.

Business owners may need to adhere to multiple privacy laws which are based on the residence of the individual whose protected data you hold, not only where you do business. Additionally, privacy legislation is being actively discussed nationally, so the principles discussed here may soon apply to many more companies.

One way or another, you are likely to be covered by privacy laws either now or soon. So, it's time to start thinking about what you need to do.

1. Understand your data. It's critical to know what data you have so you can know how to protect it and how to protect the rights surrounding that data.

2. Implement and follow a written privacy policy. Whether you are covered by the new laws or not, other legislation requires privacy policies in multiple situations, and no matter what, you should a) know how you are going to handle private, personal data, even if it's just IP addresses gathered on your website; and b) tell people what you are going to do with their data.

3. Get your information security in order. Both California privacy laws offer defenses to enforcement if you have a commercially reasonable level of Information Security in place. If your firm is large, speak with your Information Security experts to ensure that your practices comply with the law. Otherwise, make sure you have retained qualified Information Security experts to ensure you are protecting your organization. Remember Information Technologist are not Security experts, and you need to consult Information Security subject matter experts who understand what it means to have commercially reasonable Information Security.

4. Develop operational privacy management procedures. Built upon sound privacy policies, effective operational procedures ensure your ability to comply with privacy laws and other contractual responsibilities.

Business owners may need to adhere to multiple privacy laws which are based on the residence of the individual whose protected data you hold, not only where you do business.

Privacy laws are here and will only get stronger. From a privacy perspective, you must ask: Are we employing commercially reasonable levels of privacy and protection now and if new laws are passed – will we still be covered? If the answer to either is 'no,' it's time to get ready.

David Lam, CISSP, CPP, is partner and CISO at Miller Kaplan. Learn more about the firm's information security services at millerkaplan.com.