CALIFORNIA'S CONSUMER PRIVACY ACT AND THE FUTURE OF PRIVACY IN THE U.S.

How California continues to lead the way in privacy protection

BY BRETT LOCKWOOD

CALIFORNIA led the way over 15 years ago when, in 2003, it implemented the first state data breach notification law in the United States. Since that time, concerns about data privacy and cybersecurity have increased so notably among consumers and businesses that now all 50 states have some form of data breach law. These laws are in addition to numerous other state and federal regulations concerning the secure handling of personal data, as well as the far-reaching and recently effective European General Data Protection Regulation (GDPR).

Against this backdrop, California continued its trailblazing approach in this sensitive area of the law by enacting its Consumer Privacy Act (CCPA, or the "Act") this past June. The CCPA's extensive requirements will impose significant new data privacy requirements on ▶

The Act potentially impacts many U.S. businesses, given California's large population and the extensive sales made to California consumers by businesses located elsewhere.

covered businesses – including many businesses located outside of California – and likely portends similar legislation in other states as well as at the federal level.

Amendment Process and Effective Date

The CCPA was enacted by the California legislature at the beginning of the summer of 2018 with breakneck speed to forestall a ballot initiative that was then planned for the fall. Given its hasty passage and the complexity of its provisions, the final bill contained numerous provisions that were ambiguous and in need of further clarification. To address some of these concerns, the legislature enacted a handful of clarifying amendments in August. However, these amendments still left many aspects of the Act unclear. Before the January 1, 2020 effective date for the Act, the state legislature may enact further amendments, and the state attorney general is also expected to issue related clarifying regulations. Because of the recognized need for additional guidance for businesses and consumers affected by the Act, there is a grace period on enforcement actions, which runs from the earlier of (i) six months from the issuance of required regulations by the attorney general or (ii) July 1, 2020.

The CCPA's Requirements

Fundamentally, the CCPA is intended to further the personal right to privacy under the California Constitution. To accomplish this, the CCPA provides several practical means for California residents to assert greater control over personal information collected about them. Thus, under the law, California consumers have the following additional rights:

- The right to know what personal information is being collected about them by covered businesses
- The right to know whether their personal information is sold or disclosed and to whom
- The right to stop the sale of personal information
- The right to have collected personal information deleted
- The right not to be discriminated against for exercising these new rights.

For each of these rights, the Act requires covered businesses to provide specified notices to consumers about these rights and to do so in a prescribed manner in the company's privacy policy and elsewhere on its website. Consumers must be provided at least two means of making requests to exercise their rights under the Act, including at a minimum a toll-free phone

number and a website address for such requests. If a consumer makes a valid request under the CCPA, the company must, without charge, promptly comply within 45 days of the request (which period may be extended for up to 90 days due to the complexity or nature of the request). When a request is fulfilled it must be done by including specific information or categories of information as detailed in the Act.

Special opt-in requirements are imposed for the sale of information for children. A business wanting to collect and sell information about a child between the ages of 13 and 16 must first obtain the child's consent. Parental or guardian consent is required for children younger than 13.

Absent the applicability of some limited exceptions, the failure to comply with the Act's requirements exposes the business to civil penalties. Penalty amounts are up to $2,500 for unintentional violations and up to $7,500 per intentional violation for actions brought by the California attorney general. Private rights of action, which can be asserted on a class basis, are also allowed for violations of the data breach portions of the Act. A business that experiences an incident of unauthorized access or disclosure of unencrypted or unredacted personal information as a result of that business's negligence risks statutory fines of between $100 to $750 per violation or actual damages incurred, if higher. If a business cures the violation within 30 days of a specified written notice, however, any related private right of action is preempted.

Covered Businesses and Exceptions

A covered business under the Act is a for-profit entity that does business in California and collects personal information of California consumers and that meets at least one of the following thresholds: (i) it has at least $25 million in annual revenue, (ii) it handles personal information of at least 50,000 consumers, or (iii) at least 50 percent of its annual revenue is derived from selling consumers' personal information. The purpose of these three thresholds is to minimize the compliance burden on smaller companies unless they are engaged in the data brokerage business. While the Act does not define what is meant by "doing business in California," that clause, and, therefore, the Act as a whole, potentially implicate many businesses throughout the U.S., given California's large population and the extensive sales made to California consumers by many businesses located elsewhere.

The Act exempts from its coverage the handling of personal information by a small number of regulated businesses if the uses of such information are within the scope of the applicable regulatory scheme. This includes health care covered entities under HIPAA, consumer credit reporting agencies under the federal Fair Credit Reporting Act, and banks and financial services companies under the Gramm-Leach-Bliley Act. However, if any of these regulated businesses use the personal information outside the scope of the regulated purposes, then such businesses and those nonexempt uses are subject to compliance with the requirements of the Act. ▶

Some have referred to CCPA as "GDPR Lite" because of the extensive rights it gives California consumers to control the handling of their personal information.

All of these laws together with the GDPR and the CCPA reflect a trend toward greater accountability for businesses for the manner in which they handle and use consumer data.

Relationship to Other Laws

Some have referred to CCPA as "GDPR Lite" because of the extensive rights it gives California consumers to control the handling of their personal information. While some comparisons to the GDPR are apt, such as the reliance that both laws place on disclosure of certain practices to affected individuals, there are also notable differences between the two laws. In some respects, the CCPA goes further than the GDPR, such as with the CCPA's much broader definition of "personal information." While the GDPR indirectly addresses data privacy, that law is more a comprehensive framework concerning data security, whereas the underlying theme of the CCPA is personal data privacy.

Other California laws already address different aspects of data privacy and cybersecurity. For instance, website operators and other businesses already are required to notify California consumers of their right to be informed about business-related disclosures of information concerning those consumers. California also has had in place a limited personal data erasure law applicable to minors that is akin to the so-called

"right to be forgotten" that has taken root in Europe. Also, as already mentioned, California has long had a robust data breach notification law. The Act adds an additional layer of restrictions and compliance alongside these existing laws. All of these laws together with the GDPR and the CCPA reflect a trend toward greater accountability for businesses for the manner in which they handle and use consumer data.

Brett Lockwood is a partner in SGR's Corporate Practice and heads the Cybersecurity Practice. **blockwood@sgrlaw.com**.

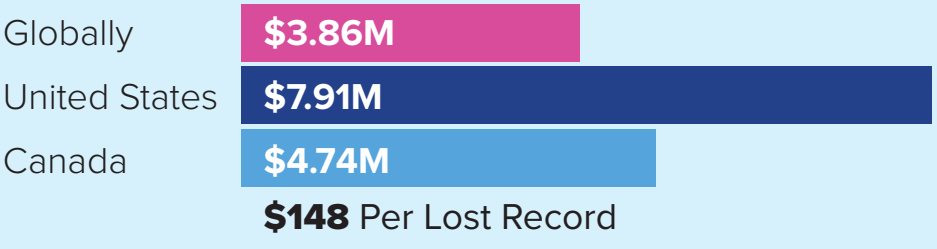
SO, WHAT TO DO NOW?

Although the effective date of the Act is January 1, 2020, and enforcement may be delayed slightly depending on subsequent regulations issued by the California attorney general, businesses should prepare for the CCPA's requirements. Among the key steps a business should undertake now are:

- **Assess what data is collected and sold concerning California consumers**
- **Implement processes to respond timely to consumer requests and to verify the identity of requesting persons**
- **Educate staff on the handling requirements under the Act and the need to be responsive to consumer requests**
- **Update its privacy policy**
- **Add appropriate links and notices on both the company's website homepage and elsewhere on its website**
- **Implement a toll-free number and other means for consumers to make requests under the Act**

CYBERSECURITY COST & RISK HIGHLIGHTS

Average Data Breach Costs



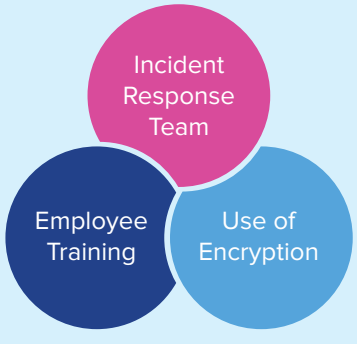
$148 Per Lost Record

Email Can Be Dangerous!

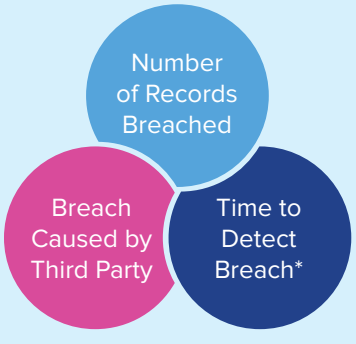
Email is the **#1 source of viruses and malware**. More than 49% of malware is installed from emails. Email content is **55% spam**. A typical user receives **16 malicious emails** each month. In the last year, **76% of businesses** reported an increase in phishing scams. The most common email "**disguises**" are:

- Bills/invoices
- Email delivery failure
- Law enforcement
- PDF attachment
- Package delivery notice
- Electronic signature notice

Major Risk Minimizers



Major Risk Multipliers



*68% took a month or more to discover

Rank of Industries as Breach Victims (By Reported Breaches)

1. Health Care
2. Hospitality
3. Public Sector
4. Retail
5. Financial Services

Percentage of Breaches Involving Employees
28%

Percentage of Above Due to Employee Error
17%
(Most incidents involve misdelivery of data or lost/stolen devices)

Sources: Ponemon 2018 Cost of Data Breach Study; Symantec 2018 Internet Security Threat Report; Verizon 2018 Data Breach Investigations Report.