BLANKROME

Cybersecurity & Data Privacy

JULY 2018 • NO.3

California Passes Historic Privacy Law: What to Consider Now to Reduce Future Financial Exposure

On June 28, 2018, California passed a historic privacy bill (AB 375) that mirrors some of the privacy obligations that recently came into effect in Europe under the General Data Protection Regulation ("GDPR"). The new California Consumer Privacy Act of 2018 (the "Act") will go into effect on January 1, 2020. The new law requires greater transparency in information practices and gives individuals powerful new rights with respect to their personal information. Complying will be a challenge for many American businesses, in particular those that have not had to grapple with GDPR.

SCOPE

- *Businesses Covered:* Generally, the Act applies to for-profit organizations doing business in California and processing personal information regarding California residents. A business is only covered by the Act if it satisfies one of the following thresholds: (a) has annual gross revenues in excess of $25 million; (b) processes for commercial purposes personal information of 50,000 or more consumers, households, or devices; or (c) derives 50 percent or more of its annual revenues from selling consumer personal information.
- *Personal Information Defined:* The Act defines "personal information" very broadly to include not only any information that identifies or can be linked with a particular consumer or household, but also information that even relates to or describes a consumer or household. It includes purchasing history, Internet, or other electronic network activity information, geolocation data, and biometric data. Web tracking data is clearly contemplated by the definition, including data that many businesses in the United States have not considered "personally identifiable" in the past.

BASIC REQUIREMENTS

- *Transparency:* In general, businesses must notify consumers regarding their personal information practices at or before the time the personal information is collected from the consumer, including notice of the categories of personal information collected and the purposes for which the personal information will be used. Companies in the United States are used to doing this for information collected online, but the Act requires that notice be provided about any personal information processed by a business, even if it is offline information.

- *Individual Rights (Including the Right to Be Forgotten):* California residents will also now have certain rights with respect to their personal information, including the right to access the information processed by a business, to obtain copies, and to have the information deleted. Individuals may also request that businesses disclose to them the categories of personal information sold to third parties or disclosed to third parties for a business purpose, and the categories of third parties that receive such personal information. Further, a third party that receives personal information may not resell the information without first notifying the individual.

- *Do Not Sell Button:* California consumers also have the right to tell businesses that they cannot sell their personal information. Businesses must facilitate this by having a clear and conspicuous link on their website that is titled "Do Not Sell My Personal Information" that enables the consumer to opt out of the sale of his or her personal information.

- *Non-Discrimination:* Importantly, a business cannot discriminate against a consumer because the consumer exercised his or her privacy rights under the Act, but the Act allows businesses to financially incentivize consumers to opt-in to its data practices, or to charge consumers a different price or provide different value if the consumer opts-in, so long as the difference in price or value is reasonably related to the value of the data.

ENFORCEMENT

The law allows the California attorney general to investigate violations and impose penalties not to exceed $7,500 per violation for intentional conduct. In addition, consumers have a privacy right of action under the law. Damages paid by businesses cannot exceed $750 per person in each instance where the law is violated. The Act also authorizes a privacy right of action for data breaches involving personal information under California's data security law without proof of harm. A suit can be brought by a consumer if there is an unauthorized access, exfiltration, theft, or disclosure of his or her unencrypted personal information as a result of a business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the business. Statutory damages under this section are not less than $100 or greater than $750 per consumer per incident, or actual damages, whichever is greater.

THINGS TO CONSIDER NOW

While the law does not go into effect until 2020, companies that operate in California or nationwide should pay close attention to developments with respect to the Act. Companies should not wait until the last minute to come into compliance because, as with GDPR, it will take real time and effort to comply.

- Conduct a data inventory to understand what personal information you collect or receive, the purposes for which you process the personal information, and any third parties with whom you share the personal information. Maintaining a current data inventory creates a solid footing to comply with any privacy law.

- Create a data map to understand where personal information resides within your organization. If an individual requests access to his or her personal information or exercises his or her right to be forgotten, knowing where personal information resides within the organization will be critical to respond within the required timeframes.

- If your business must comply with GDPR, consider whether there are benefits to applying your GDPR policies and procedures to your U.S. business operations. Many companies in the United States took the approach of treating EU residents differently from U.S. residents to take advantage of more lenient privacy requirements in the United States. Once the Act goes into effect in California, it may be an administrative challenge to separate how you treat California consumers from how you treat consumers from other parts of the United States, and other states may ultimately follow California's lead. So, it may be most efficient to simply apply your GDPR processes to the entire business in the United States. Further, there is likely a public relations benefit to treating all consumers the same in terms of their privacy rights.

- Review your insurance. Many companies have cyberinsurance, but cannot presume that their current cyber policy will protect against unique exposures arising out of the Act. For example, the Act allows for regulatory fines or penalties for failures to comply. Many cyber policies cover regulatory exposures, but only with respect to proceedings addressing failures to protect private information. However, regulators may pursue companies under the Act for broader noncompliant data collection

and use practices. Thus, current regulatory coverage may not be sufficient to protect against Act regulatory events. Similarly, many current cyber policies cover amounts spent by companies when private information has been breached or improperly accessed. But, not all policies cover claims or lawsuits against your company by individuals claiming noncompliance with broader data use restrictions imposed by the Act, particularly when such noncompliance does not result in a data breach. And, as with GDPR, where insurers have added "GDPR" language or endorsements to their policies that did not in all instances provide actual GDPR-related protection, endorsements purporting to address the Act may not provide as much protection as anticipated. Thus, as companies are purchasing/renewing cyber policies in advance of the Act becoming effective, they should carefully scrutinize policy language to ensure that the correct language is included to fortify insurance protection against unknown future financial exposures.

For additional information, please contact:

Jennifer J. Daniels
Cybersecurity & Data Privacy Group Leader
212.885.5575 | daniels@blankrome.com

Linda Kornfeld
424.239.3859 | lkornfeld@blankrome.com