BCLP. Client Intelligent

Insights

THE EXPANDED PRIVATE RIGHT OF ACTION UNDER THE CPRA

Dec 03, 2020

On November 3, 2020, Californians voted to pass Proposition 24, expanding and modifying the California Consumer Privacy Act ("CCPA"), which came into force on January 1, 2020. The new California Privacy Rights Act ("CPRA"), supersedes the CCPA and will be operative on January 1, 2023 (with a look-back period starting January 1, 2022). Until that time, the CCPA as currently written remains in effect. As we learned during the lead up to the CCPA, the time period to prepare for this type of comprehensive and complex legislation passes quickly, and companies need to begin their CPRA preparations sooner rather than later. In the first of our CPRA series, we discuss the expansion of the scope of the CCPA private right of action and its implications for organizations trying to anticipate the impact of the CPRA.

The CPRA expands the current CCPA private right of action (CA Civil Code Section 1798.150(a)(1)) by authorizing consumers to bring lawsuits arising from data breaches involving additional categories of personal information. Specifically, the CPRA adds email address in combination with a password or security question and answer that would permit access to the consumer's account to the list of data types that can be actionable under the law in the event of a breach.

Currently, the private right of action is tied to the categories of personal information that trigger a breach notification obligation under California law rather than the broader definition of "personal information" set out in the CCPA. While the California breach notification statute can be triggered by a breach of email addresses in combination with a password or security question and answer, this additional category was not initially included in the CCPA private right of action section. This means that, in most cases, breach of mere login information for an account which does not provide access to payment/financial information or health information or similar categories of personal information would not trigger the ability of a consumer to seek statutory damages (either individually or part of a class action). As of January 1, 2023, that will no longer be the case.

The impact of this amendment on future litigation is also certain to be significant, as many data breaches involve the disclosure of email and password/security question and nothing else or nothing that would trigger a breach notification obligation under California law. This information is widely available on the dark web and also is often reused by consumers, making credential stuffing

and related tactics particularly effective tools for gaining access to consumer accounts. Consequently, it seems inevitable that there will be a sharp rise in class action litigation as plaintiff's attorneys and consumers make claims for statutory damages available under this provision rather than looking for situations that would likely be successful under more traditional but less certain tort claims. With potential statutory damages ranging from $100 to $750 per consumer per incident and breaches often involving hundreds of thousands or even millions of users, these types of claims could be staggering for companies.

With this significant change on the horizon, it will be more important than ever for companies to continue to evaluate their security controls, retention practices and processes, and incident response programs as well as the scope of related cyber-insurance to make sure that they are prepared. The more equipped companies are to prevent breaches as well as to respond and mitigate incidents, the lower the overall risks will be in spite of the expansion.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Partner; Chair – Global Data Privacy and Security Practice; and Global Practice Group Leader – Technology, Commercial & Data, Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.