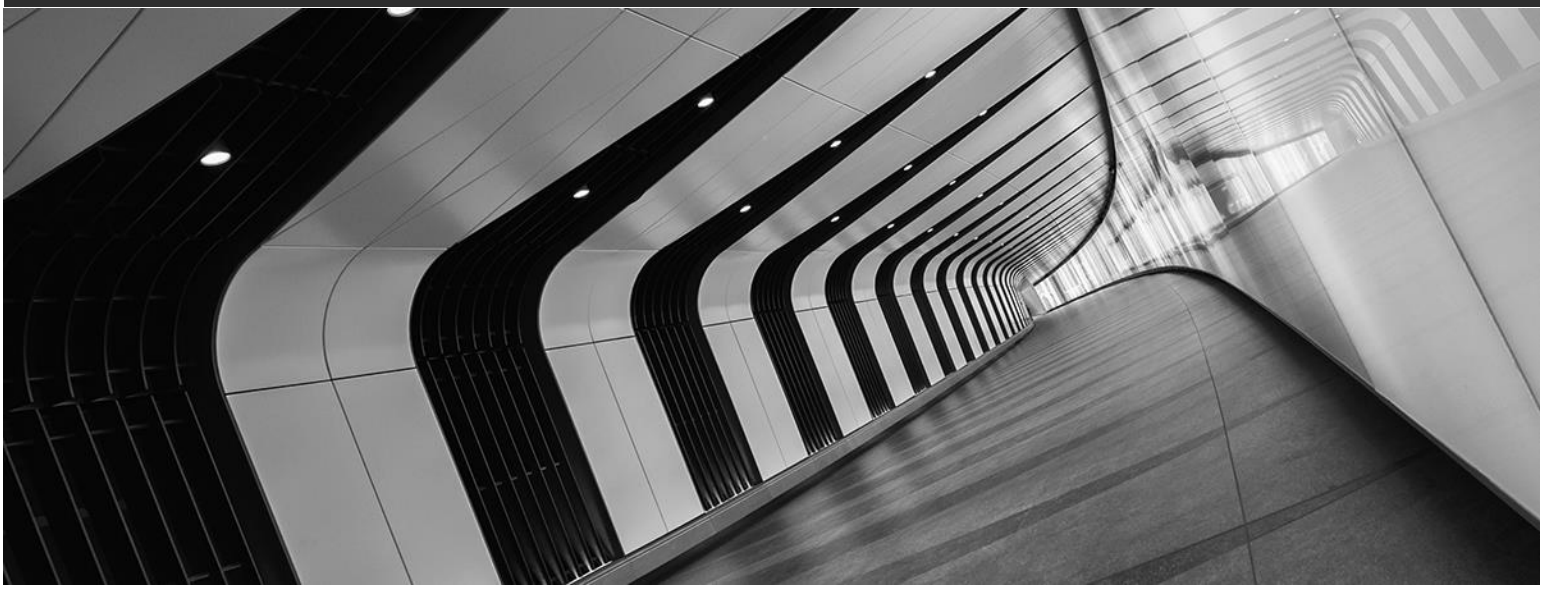
GT GreenbergTraurig

Anticipating the Flood of Cybersecurity Litigation Under the CCPA—What to Do About It



The CCPA is extremely broad in scope compared to other U.S. privacy laws; it applies to the use of personal information about California residents—rather than regulating the use, collection and dissemination of information obtained by companies from consumers.

By Ian Ballon and Rebekah Guyon | January 25, 2019 | The Recorder

Unless amended by the legislature, modified by regulations to be promulgated by Attorney General Xavier Becerra, or pre-empted by federal legislation, the California Consumer Privacy Act, Cal. Civ. Code Sections 1798.100 et seq. (CCPA), which is set to take effect on Jan. 1, 2020, will invite an explosion of class action litigation, as plaintiffs counsel seek to recover statutory damages between $100 and $750 for each California resident affected by a security breach.

The CCPA is extremely broad in scope compared to other U.S. privacy laws; it applies to the use of personal information about California residents—rather than regulating the use, collection and dissemination of information obtained by companies from consumers. The CCPA confers on California residents the right to be notified of the personal information collected from them and the purpose of the

collection, request disclosure of the specific personal information that a business has collected from them, opt out of the collection of their personal information, and demand that their personal information be deleted. The CCPA mandates that businesses place specific notices regarding residents' rights under the law on their websites, amend their privacy policies, require their service providers to adhere to the CCPA, and adjust internal practices and procedures to ensure compliance. While the law excludes businesses with annual gross revenue below $25,000,000 that do not buy, sell or receive for commercial purposes personal information of 50,000 or more consumers, households or devices or derive 50% or more of their annual revenue from selling consumers' personal information, it will apply to thousands of companies inside and outside the state that use the personal information of California residents. The law also contains many gaps and unexplained provisions that presumably will be resolved by subsequent amendment of the legislature, regulations that will be promulgated on or before Jan. 1, 2020, or though regulatory enforcement actions by the California Attorney General.

The good news for companies is that most of the CCPA's provisions will be subject only to regulatory enforcement actions, not civil litigation. Unfortunately, however, the narrow right to a private cause of action created by the CCPA will encourage plaintiffs lawyers to file suit virtually every time a security breach exposes the unencrypted or unredacted information of California residents, given the availability of potentially large statutory damage awards. One need only look to the experience of companies defending litigation under other statutes that provide for statutory damages such as the TCPA to see how the CCPA will impact companies if it takes effect as currently drafted and is not preempted by federal law.

The CCPA creates a private cause of action for the "unauthorized access and exfiltration, theft or disclosure" of a California resident's "nonencrypted or nonredacted personal information" "as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information," see Cal. Civ. Code 1798.150(a)(1). At first blush, this provision may sound sensible—it only applies to breaches that result from the failure to maintain "*reasonable*" security measures. But "reasonable" security measures are not defined in the CCPA. Other provisions in the statute may evidence the legislature's intent for "reasonable" security measures, such as the CCPA's definition of "deidentified" information (which is not "personal information") by reference to the "technical safeguards" and "business processes" that a business must implement to prohibit and prevent against reidentification. Presumably "reasonable security procedures and practices" could include technical safeguards and business processes protecting against security breaches. Ultimately, what is or isn't reasonable would be determined by judges and juries based on the facts of a given breach.

The statutory damages potentially available under the CCPA will likely provide strong motivation for the plaintiffs class action bar to test its scope. Under the CCPA, California residents may recover the "greater" of actual damages or statutory damages of "not less than" $100 and up to $750 per consumer per

incident, in addition to injunctive, declaratory, or "any other relief the court deems proper," Cal. Civ. Code Section 1798.150(a)(1)(A) – (C). A court has wide discretion to consider any "relevant circumstances presented by any of the parties" in assessing the amount of statutory damages, including factors such as the seriousness of a business's failure to implement and maintain reasonable security measures, the length of time that it failed to do so, willfulness of a business's misconduct, and the business's assets, liabilities, and net worth. Depending on the nature of the business and the breach, these considerations may mitigate the most extreme awards.

Nonetheless, the availability of substantial statutory damages for even a negligent failure to prevent a security breach by a malicious third party is extraordinary. A putative class action lawsuit involving 100,000 state residents could claim up to $7.5 million in statutory damages. A successful lawsuit involving 1,000,000 consumers could result in an award of up to $750 million and in any case no less than an award of $100 million. These damage calculations are vastly disproportionate to actual damages in most security breach cases. In the typical cybersecurity class action suit consumers who have not been the victim of identity theft or financial fraud typically have not incurred any financial harm. Yet based on the availability of statutory damages, businesses potentially could be forced into bankruptcy in cases where a class action is certified and liability established.

A California resident may only initiate a suit for statutory damages, whether individually or as a putative class action, after giving a business notice and a 30-day opportunity to cure its failure to maintain reasonable security measures, Cal. Civ. Code Section 1798.140(b). This provision tracks the 30-day notice and cure period in the California Consumer Legal Remedies Act, a statute popular with class action counsel, some of whom have become adept at asserting claims for which a "cure" realistically is not possible, Cal. Civ. Code Section 1782. Indeed, it is unclear how, if at all, a security breach that has already occurred can be *cured*. The CCPA seems to acknowledge that possibility in framing this prerequisite to suit as limiting the statutory damage remedy only "[i]n the event a cure is possible …" Cal. Civ. Code Section 1798.150(b). The ability to cure is also not a guarantee against a lawsuit; if a business is able to cure the breach, it must provide an express written statement of its cure to the consumer, which itself could serve as grounds for a lawsuit and support a claim for statutory damages if the business violates its own promise to cure.

The CCPA includes a novel state regulatory regime, empowering the California Attorney General to pass regulations "to further the purposes" of the act, Cal. Civ. Code Section 1798.185, akin to the Federal Trade Commission's authority to issue implementing regulations under certain privacy laws or proscribing unfair competition, see 15 U.S.C. Section 57a. It remains to be seen whether Becerra, who has begun holding public meetings on the rule-making process, will elaborate on the type of "cure" that would satisfy the CCPA and the meaning of "reasonable" security measures, or whether the state legislature takes action in further amendments to the CCPA before the law takes effect. It also remains to be seen whether

Congress will enact a federal statute that preempts the CCPA, as it did sixteen years ago when it enacted the CAN-SPAM Act in part to prevent an overly burdensome state anti-spam law from taking effect in California.

If the CCPA's litigation provisions take effect as currently drafted, the availability of potentially punitive statutory damage awards may usher in a litigation explosion that will harm companies that do business with California residents. To limit their risk of exposure, businesses should consider entering into binding arbitration provisions in enforceable contracts with consumers. To the extent a business is engaged in interstate commerce, the Federal Arbitration Act would require courts to enforce arbitration of CCPA claims. See, e.g., *AT&T Mobility v. Concepcion*, 131 S. Ct. 1740 (2011). To maximize enforceability, businesses should also include enforceable delegation clauses, to minimize the opportunity for judges hostile to arbitration to defeat the enforceability of arbitration clauses. See, e.g., *Henry Schein v. Archer & White Sales*, _ U.S. _, 2019 WL 122164 (U.S. Jan. 8, 2019); *Rent-A-Center, West v. Jackson*, 130 S. Ct. 2772 (2010); see generally Ian C. Ballon, "E-Commerce and Internet Law: Legal Treatise with Forms" 2d ed. Section 22.05[2][M] (West 2008 & 2019 Cum. Supp.).

Businesses also should take steps to keep personal information in encrypted or redacted form to avoid the scope of the law.

Businesses that fail to take these steps, and which possess the personal information of California residents that is unencrypted or unredacted—including many out of state companies—may find themselves subject to potentially crippling liability in the event of a cybersecurity breach in cases where a class action is certified.

About the Authors:

Ian Ballon *has served as lead counsel in successfully defending numerous cybersecurity breach and data privacy class action suits. He is co-chair of Greenberg Traurig's global intellectual property and technology practice group and a litigation shareholder in the firm's Silicon Valley and Los Angeles offices. He is also the author of West's five-volume treatise, E-Commerce and Internet Law 2d edition (www.ianballon.net), which he updates annually "in his spare time." He may be reached at Ballon@GTLAW.com.*

Rebekah Guyon *is a litigation attorney in the firm's Los Angeles office. Her practice focuses on defending cybersecurity and data privacy class action suits and in representing clients in technology, entertainment, and intellectual property litigation. She may be reached at GuyonR@GTLAW.com.*