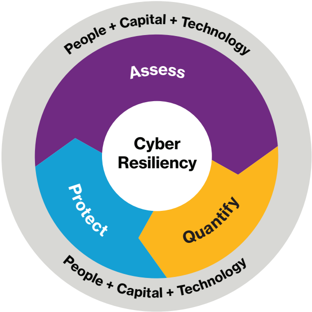
Decode regulation.



Changing exposures and risks posed by the Consumer Privacy Act: What you need to know and what lies ahead

By Ashley L. Hart, Donna Wilson, Linda Kornfeld and Brandon Reilly

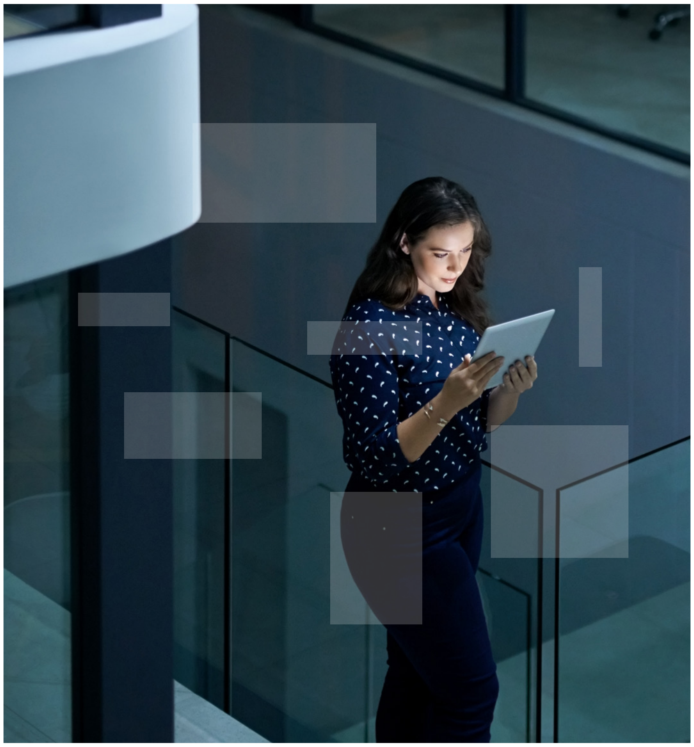
With the cybersecurity landscape constantly evolving and changing, the pressure to protect consumer privacy rights is increasing. A reflection of this concern is the California Consumer Privacy Act (CCPA). While the CCPA is not effective until January 1, 2020 at the earliest, it is important for businesses to evaluate the CCPA's potential risks and exposures alongside their own current privacy and data security policies.

A Californian privacy law seems to appear out of thin air

You can be forgiven, if the feverish buildup to the May 25, 2018 deadline for compliance with the European Union's General Data Protection Regulation (GDPR) made you miss the announcement of the California Consumer Personal Information Disclosure and Sale Initiative in late 2017. The campaign to use California's unique ballot initiative system to create an omnibus privacy law began relatively quietly, but before we knew it, the initiative's proponent, real estate developer Alistair MacTaggart, had submitted double the signatures required to qualify for the November ballot and in the same month that GDPR went online.

What happened next was a hurried attempt by legislators, privacy advocates, and business interests to address the concerns that gave rise to the initiative before it was placed on the ballot. In a matter of only a few weeks, state legislators raced to draft a legislative version of the initiative in time for the June 28 ballot deadline, the date after which ballot initiatives are locked for November. Prior to that date, MacTaggart and his campaign retained the discretion to withdraw the initiative in favor of an acceptable legislative alternative. A deal was reached on June 22, and the CCPA was passed and signed by Governor Jerry Brown just before the June 28 deadline.

> **Due to its expedited passage, the CCPA arguably contains many apparent ambiguities, redundancies, and outright contradictions.**



So-called 'technical fixes' were implemented in a September 2018 amendment, which included, among other things, a pushed back deadline for the primary requirements to 2020, and clarifications regarding certain provisions, such as the HIPAA exemption.

As it currently stands, the CCPA broadly applies to for-profit businesses that process the data of California residents; and have either annual revenues exceeding $25 million, obtained the personal information of 50,000 or more California residents annually, or derived over half of their annual revenue from selling California residents' personal information.[1] Nuanced exemptions exist for various federally regulated industries to the extent they process personal information protected by HIPAA or GLBA.[2]

The CCPA enshrines several new consumer privacy rights into law. These can be understood as the law's 'primary rights' such as the right to access information, the right to deletion, and the right to opt-out of data sales. Further protections are also present and are known as 'associated rights,' such as comprehensive requirements for privacy policy notifications, a mandate that consumers cannot be discriminated against for exercising their rights, and a right to data portability. These privacy provisions are enforceable only by the California Attorney General with a statutory penalty between $2,500 and $7,500 per violation, subject to a 30-day right to cure, the parameters of which are unclear.

Raising the stakes of data breaches

Standing out among the CCPA's new liability provisions is the law's landmark private right of action for statutory damages as a result of a data breach arising from a failure to follow reasonable security practices. The provision allows consumers to recover the greater of $100 to $750 per incident or actual damages, subject to a 30-day right to cure. The availability of statutory damages represents a potentially dramatic departure from existing remedies for data breaches.

To give you an idea of the immense scale of these new penalties, consider the recent national settlement of a 2016 breach that allegedly was not revealed until late 2017. The $148 million settlement has been billed by the New York attorney general as the largest ever multi-state data breach settlement, yet, under even the minimum statutory penalties provided by the CCPA, this record would be dwarfed for California users *alone*. If we assume that 12 percent, which is the approximate share of Californians in the U.S., of the company's 20 million customers affected resided in California, the company would have faced a minimum penalty of **$250 million** and a maximum penalty of **$1.8 billion.**

Importantly, a business is now provided an opportunity to 'cure' alleged breaches within 30 days of receiving notice of potential claims.[3] The safe harbor applies if the business 'actually cures the noticed violation' and provides the claimant with 'an express written statement that the violations have been cured and that no further violations shall occur'.[4] But what constitutes a sufficient 'cure' for a data breach? Is it an assurance that no fraud has resulted from a suspected breach incident? A business may attempt to prove that stolen data was returned, bad actors were detained, or the suspected vulnerability was patched. But the adequacy of the 'cure' may itself be subject to costly and protracted litigation.

Get ready for debates

The new breach provision potentially creates some awkward incongruities with existing California law because it appears both broader and narrower than the state's data breach notification law (DBNL), which appears to stand unaltered by the CCPA's passage. The CCPA is arguably *broader* because it appears to make actionable incidents that do not necessarily involve unauthorized acquisition. Specifically, the law applies where personal information has been 'subject' to 'unauthorized access and exfiltration, theft, or *disclosure*'.[5] It is unclear whether the legislature intended to cover disclosure to an unauthorized individual, or a subsequent disclosure from that individual, which would seemingly require 'exfiltration' or 'theft' as an initial step. Nonetheless, plaintiffs and others can be expected to argue that the standard is broader than the DBNL, which is applicable only where personal information has been 'acquired by an unauthorized person'.[6]

The CCPA is also *narrower* because it imposes a standard of care that is missing from the DBNL. Under the CCPA, a breach is only actionable when it is the result of the business' 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'.[7] The DBNL contains no such limitation.

The result of this misalignment is that businesses could be faced with the following situations, at least in theory:

1. A business has sent data breach notification letters to California consumers, yet a CCPA cause of action does not lie because the incident was not the result of a breach of 'the duty to implement and maintain reasonable security procedures and practices'

2. A business is exposed to a CCPA cause of action for an incident in which no notification was required or given because the incident involved mere unauthorized access, and there was no evidence of unauthorized acquisition or theft

Also up for debate is what California legislators really mean when they say ’reasonable security procedures and practices’. Where does the language come from? The provision borrows language from the California Records Act, initially implemented in 2004, which requires covered businesses to ’implement and maintain reasonable security procedures and practices appropriate to the nature of [personal information about a California resident], to protect the personal information from unauthorized access, destruction, use, modification, or disclosure’.[8] That requirement, like the DBNL, is enforceable by private right of action ’for damages’ but does not provide for statutory damages.[9]

There appears to be some uncertainty as to what ’reasonable security procedures and practices’ actually means. In the *LabMD v. FTC* decision, the Eleventh Circuit vacated a 2016 consent order between the FTC and LabMD that required the company to ’implement and maintain a reasonable data security program’[10] The court found that this standard required ’an indeterminable amount of reasonableness’ because it ’does not enjoin a specific act or practice’ or ’instruct LabMD to stop committing a specific act or practice’. Rather, the consent order ’mandates a complete overhaul of LabMD’s data security program and says precious little about how this is to be accomplished’. As a result, the court concluded, the command was unenforceable.

Potential impact on cyberinsurance policies

According to a recent study conducted by ESI ThoughtLab and sponsored by Willis Towers Watson and other organizations specialized in cybersecurity and risk management, most companies (80%) have at least a small amount of cybersecurity insurance. As such and has been the case with the passage of GDPR, businesses should review their cyberinsurance policies now to determine whether they would provide adequate protection for CCPA-related exposures. For example, some cyber policies cover loss incurred in connection with an actual breach event, but may not cover exposure under the CCPA for failures to adequately maintain, use, or delete private information. Additionally, cyber policies may contain a limited definition of personally identifiable information (PII). The CCPA contains an inordinately broad definition of personal information that may exceed that covered by the cyber policy, at issue. The CCPA statutory damages also may fall outside of a narrowly tailored definition of covered loss. Thus, policyholders should carefully review policy coverages and definitions in an effort to confirm matches between their CCPA-related risks and the insurance that they purchase.

Further, CCPA’s private right of action for statutory damages as a result of a data breach is likely to result in an uptick in data breach lawsuits. Regulatory exposure may also be significant. Under cyberinsurance policies, the policy limits can be eroded with defense and indemnity costs. As such, what may have been previously considered to be adequate policy limits before both GDPR and the CCPA, may no longer be sufficient to cover increased exposure. Policyholders should confer internally and with their insurance brokers and counsel to evaluate whether they have sufficient policy limits to defend and settle or pay judgments or fines in connection with CCPA-based proceedings. Finally, if a policyholder is faced with a CCPA proceeding, given the potential for significant exposure, it will be important that the policyholder be permitted to work with trusted expert vendors and counsel. Policies should be negotiated up front to obtain insurer concurrence regarding the retention of trusted expert vendors and counsel and confirmation that the services that they are providing will be covered under the policy.

What’s next

The September amendments to the CCPA were almost certainly not the last. Pressure seemingly exists from all sides to ’fix’ the law: Attorney General Xavier Becerra has expressed that his office faces ’serious operational challenges’ in ramping up its sole enforcement and rulemaking authority. Commercial interest groups have lobbied to raise the applicability thresholds and loosen certain provisions; and consumer rights groups would like to see a more expansive private right of action, among other things. Other likely developments include rulemaking from Mr. Becerra’s office in late 2019 or early 2020, and litigation over various potential ambiguities.

These developments could be less meaningful if a federal privacy law with preemptive power is cobbled together in Washington. In August, the *New York Times* reported that major Big Tech firms were lobbying the Trump Administration to begin outlining a federal privacy law that would preempt the CCPA. In late September, the Senate held two days of committee hearings with testimony from the chief executives of those same companies, with many appearing to endorse a new federal law amid objections to the reach of the GDPR and the CCPA.

Two bills introduced in November may give an idea about what such legislation could look like. The first bill, introduced by Senator Ron Wyden (D-OR) on November 1, proposes GDPR-like protections that were headlined by the bill's inclusion of penalties of up to 20 years in prison for responsible executives and four percent of annual gross revenue in fines. The second bill, proposed by Intel on November 6, similarly gives the FTC enforcement authority and requires annual reporting, but attempts to protect business interests by excluding civil actions, capping fines at $1 billion, and moving away from the data minimization principles reflected in the CCPA, among other things.

Conclusion

The CCPA presents increased risk to most businesses due to its novel standards, potential inconsistencies and ambiguities, and of course, its allowance for significant statutory damages and a private right of action for alleged data breaches.

By the earliest possible time of the CCPA's implementation in January 2020, a federal law with preemptive power may well be on the horizon, making any future amendments to CCPA less meaningful. However, if that is not the case, cyberinsurance policies may have already addressed CCPA-related exposures impacting coverage. Only time will tell.

Contact

Ashley L. Hart
Willis Towers Watson
+1 212 915 7477
ashley.hart@willistowerswatson.com

Donna L. Wilson, Chair, Privacy & Data Security Practice
Manatt, Phelps & Phillips, LLP
+1 310 312 4144
dlwilson@manatt.com

Linda Kornfeld
Blank Rome
+1 424 239 3859
lkornfeld@blankrome.com

Brandon Reilly
Manatt, Phelps & Phillips, LLP
+1 714 338 2701
breilly@manatt.com

Sources

[1] Cal. Civ. Code § 1798.140(c)(1).
[2] Cal. Civ. Code § 1798.145(e).
[3] Cal. Civ. Code § 1798.150(b).
[4] *Id.*
[5] Cal. Civ. Code § 1798.150(a)(1).
[6] Cal. Civ. Code § 1798.82(g).
[7] Cal. Civ. Code § 1798.150(a)(1).
[8] Cal. Civ. Code § 1798.81.5(b).
[9] *See* Cal. Civ. Code § 1798.84(b).
[10] *LabMD, Inc. v. Federal Trade Commission*, 894 F.3d 1221 (11th Cir. June 6, 2018).

WTW-NA-2019-WTW163861
willistowerswatson.com