

Potentially Expanded Private Right of Action Increases Risk of Class Action Exposure Under the California Consumer Privacy Act

May 1, 2019

Looking Back - the California Consumer Privacy Act, and How We Got Here

As companies were getting up-to-speed on the effects of the European Union's General Data Protection Regulation (GDPR) last year, California quickly enacted its own privacy law, the California Consumer Privacy Act ("CCPA" or "Act") last June. We address below the high risk associated with the CCPA and its interaction with regulations in key U.S. industries.

The fast-passed legislation was designed to avoid a November 2018 ballot initiative on the subject, and was plagued by errors and ambiguities that require robust clarification. The Act's take-away, however, was abundantly clear – California consumers have a right to know what personal data companies are collecting and are empowered to bring a private right of action for a data breach (and even potentially for other violations of the Act).

As the broadest-sweeping privacy legislation the United States has seen in 20 years, the Act quickly spun off numerous state equivalents, including [Hawaii \(S.B. 418\)](#), [Maryland \(S.B. 613\)](#), [Massachusetts \(S.D. 341\)](#), [New Mexico \(S.B. 176\)](#), [New York \(S.B. 224\)](#), [Rhode Island \(S.B. 234\)](#), and [Washington \(S.B. 5376\)](#), among others. Even with so many states on the privacy bandwagon, federal preemption is unlikely in the near future given disagreements around the mechanisms of enforcement, the types of data deserving protection, and conflicting incentives for companies versus consumers.

While the legislation itself is cumbersome, we broke it down in detail for you [here](#). At brass tacks, consumers now have a right to know which of their personal information has been collected and shared, can opt out of the sharing of that personal information, and can request deletion of same. The threshold for compliance for companies is three-fold: 1) gross annual revenues over \$25 million, 2) buy, receive, sell, or share the personal data of 50,000 or more consumers, households, or devices, **or** 3) receive at least 50% of annual revenue from selling consumers' data. Importantly, a covered company need

Related Capabilities

- Privacy & Social Media
- Trademark, Copyright + Advertising
- Technology Commerce
- Technology

meet only one of the three criteria.

With such a broad breadth, the Act's coverage spans companies across all industries.

Industry Spotlight - What's the Impact to Your Company?

The stated goal of the CCPA is simple—to give California residents control over how their personal data is used, stored, and sold. From a consumer perspective, this sounds desirable enough. That is, until you look a bit under the cover at how compliance is going to be effectuated from an industry perspective.

Health Care Industry

For the health care industry, exemptions are key. However, any health care company with employees in California, or that operates a website accessed by California residents, will likely be covered. In terms of types of information covered, industry insiders should keep a careful inventory of consumer personal information to help meet one of the Act's carve-outs for protected health information collected by HIPAA-regulated "covered entities" and "business associates." A HIPAA-governed entity or Confidentiality of Medical Information Act ("CMIA")-governed health care provider can obtain an exemption for patient information maintained in the same manner as medical information or protected health information.

Notably, the HIPAA and CMIA exemptions apply not to the covered entities themselves, but instead to the information collected by the entities. To the extent covered entities and health care providers maintain information not governed by either HIPAA or the CMIA, they might still be required to comply with the Act's provisions relating to the collection, use, and sharing of that data. Thus, health care businesses must pay careful attention to the types of information they are collecting, how that information is defined across different statutes, and the extent to which similar data receives dissimilar protection under the idiosyncratic definitional structure of the CCPA. For example, data that is "deidentified" under HIPAA, and therefore no longer considered protected personal health information, may not qualify for protection under the CCPA's carve-out, creating potential compliance gaps and litigation risk.

Food and Agriculture Industry

Compliance is comparatively easier for the food and agriculture industry because of the types of data collected. AgTech businesses, which are plentiful in California, typically do not collect an abundance of personally identifiable information. However, if they have employees in California, operate a website used by California residents, or use precision agriculture tools to collect information about individual producers, such as names, addresses, or social security numbers, they will be required to comply with the CCPA. Thus, it will behoove AgTech businesses to begin their compliance work and keep careful records of the types of information they collect, since the CCPA applies to information collected both on and offline.

Financial Services Industry

The financial services industry, just as the healthcare industry, must carefully inventory information collected, since the CCPA does not apply to personal information that is “collected, processed, sold, or disclosed” pursuant to the Gramm-Leach Bliley Act (“GLBA”) and the California Financial Information Privacy Act (“CFIPA”), but likely will apply to employee information, and certain information collected from website and app users from California. Notably, the above exemptions do not immunize financial institutions from the class action data breach provisions of the CCPA. This is particularly important, given that the difference between compliance and non-compliance for financial institutions largely hinges on understanding the differences in protection that attend the treatment of similarly named, but dissimilarly defined types of data across the GLBA, CFIPA, and CCPA. For instance, both the GLBA and the CFIPA, on the one hand, and the CCPA, on the other, cover consumer and personal information; however, nuanced differences in definitions between the statutes mean that information may fall between the cracks of the financial exemptions and CCPA protection.

The consequences of such a compliance gap are more acute in the financial sector, given that class action litigation has been made available to address the “unauthorized access and exfiltration, theft, or disclosure,” of the nonencrypted or nonredacted personal information of consumers, that has been compromised as a result of the financial institution’s failure to maintain “reasonable security procedures.” Since the statutory language establishing the carve-outs for financial information does not apply to the private right of action provision, financial institutions, like all other businesses, are still on the hook for significant statutory damages in the event of a data breach.

Technology and Fintech Industry

Technology/fintech companies will need to tailor their business activities to avoid implicating restrictions on the sharing of data and reselling personal information. Under the CCPA, consumers have the right to opt out of the sharing of their personal information, and third parties to whom a consumer’s information has been sold are prohibited from re-sharing that information until the consumer has been notified of the sharing and afforded the opportunity to opt out. Given the expansive definition of “sell” under the CCPA, data-dependent companies stand to lose the very foundations of their businesses models.

Interestingly, the impact here is not exclusive to the business side. While it is certainly true that data brokers, social media platforms, and mobile application developers will acutely feel the impact of restrictions on “selling,” and “re-selling,” personal information, to the extent that their operating revenues are dependent on exactly the type of data exchange and ad networks the CCPA seems to cover, consumers, who have become accustomed to a free Internet, might be similarly impacted. If website operators can no longer fund their offerings via data exchanges and ad placement, they will be forced to solicit payment for services, potentially harming consumers who do not want to pay for content.

Thus, regardless of industry, the CCPA stands to leave a definitive footprint in how companies handle consumer data going forward and will heighten focus on consumer privacy.

What's New and Where Are We Headed?

If the broad industry impact of the CCPA isn't scary enough, the fact that the legislation itself keeps changing should spook even the most compliance-minded companies. Due to its hasty drafting, the CCPA has already been formally amended once. The California State Legislature passed SB-1121 in August 2018, amending the original legislation to address questions of enforcement, exemptions, and preemption, among other changes. However, new amendments might still be forthcoming.

For example, California Assembly Bill 25 was introduced in December to amend the Act to exclude employees from the definition of consumer. Of particular note in this space, the CCPA covers employee data, to potentially include performance reviews, internal correspondence, and other personal information germane to Californians in their roles as employees. Given the undesirable consequences of allowing the Act to cover employee data access requests (to include not only overwhelming request volume, but also misuse of the system to acquire information for use in employment lawsuits), the bill, if passed, hopes to divorce information collected pursuant to employment or application for employment from the personal information protected under the CCPA. Any benefit to be gained by the exclusion of employee information, however, would be eclipsed by the potentially enormous impact of SB 561, if passed.

The amendments proposed in SB 561, introduced in the California Legislature on February 22, 2019, by California Attorney General ("AG") Xavier Becerra and California State Senator Hannah-Beth Jackson, are significant for all industries covered by the CCPA.

The proposed changes broaden the scope of the private right of action to encompass *ALL* violations of the CCPA, as opposed to only data breaches. Importantly, the proposed amendments would also remove other business safeguards, such as the 30-day cure period during which businesses may attempt to rectify violations following notice thereof, and business' entitlement to solicit opinions from the AG regarding compliance guidance (the general guidance would instead be published).

What's the Takeaway - Why Should We Be Concerned?

As the law currently stands, the California AG cannot begin to bring enforcement actions for violations of the CCPA until July 1, 2020. However, the private right of action becomes available on January 1, 2020. As we have noted, the difference between compliance and liability for many industries is the CCPA's ambiguous and often counterintuitive definition of key terms - i.e., "consumer," "personal information," "sell," even "business," to the extent that non-profits (important in the health-care context) are roped into the CCPA's coverage if they are controlled by a for-profit entity.

An expanded private right of action would allow consumers to bring actions for violations big and small, technical and substantive, and questionably defensible, insofar as consumers may not be required to show any concrete, particularized harm in the event of a violation.

If you've been following Dorsey's coverage on the CCPA, then you know that this means \$\$\$, especially for hungry class action attorneys, as the potential for damages is high. The CCPA, as amended, permits a penalty assessed by the AG of up to \$2,500 for each unintentional violation, and up to \$7,500 for each intentional violation; for private plaintiffs in the data breach context, statutory damages range between \$100-\$750 per individual, per incident. This means that even a relatively small data breach involving 15,000 people equates to at least \$1.5 million in damages. Now imagine 25,000 people. Well, you do the math. The litigation costs alone are potentially catastrophic.

How Much Will It Cost You - Damages and Class Risk Are Key

The risks and costs of the class actions or litigation are not the only financial impacts, however. Inevitably, cyber insurance premiums will increase, investigation costs and data gathering for compliance purposes will rise, and conflicting interpretations of various provisions will be promulgated, further complicating an already oblique compliance landscape. Even attempts to outmaneuver class action liability are likely to have unintended, injurious consequences. The CCPA contains a prohibition against class action waivers; however, there is a strong argument to be made that the Federal Arbitration Act will preempt this provision. Yet, as we saw in the recent Uber arbitration case, attempts to limit class action liability by instituting mandatory arbitration provisions can backfire, where, as with Uber, mass arbitrations stick businesses with millions of dollars in filing fees alone.

Creative plaintiff's lawyers will also tack on potential liability under the California Unfair Competition Law ("UCL") if they are able to convince courts that the UCL can be used as a vehicle to pursue additional damages, or even non-data breach-related violations of the Act. The UCL prohibits businesses from perpetrating "unlawful, unfair, or fraudulent" business practices, authorizing private rights of action where there is an auxiliary violation of other laws. Thus, plaintiff's lawyers are likely to use the CCPA as a vehicle for sourcing unlawful or unfair consumer privacy practices, in order to weaponize them under the UCL, independently of a CCPA cause of action. More concerning still, the CCPA creates a private right of action for data breaches, which incentivizes plaintiff's lawyers to pile on a secondary UCL claim in the data breach context. In the event the private right of action is expanded to cover all violations of the CCPA, the risk profile increases tremendously.

How Dorsey Can Help

With a January 1, 2020 implementation deadline forthcoming, compliance-minded in-house attorneys should have begun compliance efforts now. [Dorsey's Cybersecurity, Privacy, and Social Media Team](#) has developed assessment tools and guidance on reasonable security practices and procedures to help prevent data breaches and defend

companies from the forthcoming tsunami of class actions. Learn more about the how the CCPA impacts your business by contacting us. Notably, Dorsey has partnered with leading technical security industry organizations to offer full-service advice.