Stradling
Attorneys at Law

CLIENT ALERT

December 2019 sycr.com

The California Consumer Privacy Act Is Upon Us; Here's What Your Company Should Be Doing

- The CCPA will impact most companies doing business in California, and it takes effect on January 1, 2020.
- Avoid the mistake of assuming that your business doesn't "sell" personal information. If you haven't already, start scrutinizing data flows and terms relating to digital advertising and your use of analytics and social media tools.
- Compliance requires much more than just updating your Privacy Policy, and the consequences for violations can be severe. Stradling's Privacy & Data Security group is here to help.

Authors:

Travis Brennan
Shareholder
(949) 725-4271

Ahmad Takouche
Associate
(949) 725-4153

The California Consumer Privacy Act of 2018 takes effect on January 1, 2020. It's the first data privacy law of its kind in the U.S., because unlike federal private-sector laws regulating privacy, it isn't limited to a particular industry. The CCPA's scope is staggering; forget the traditional, narrow definitions of personal information deserving of legal protection. In addition to sensitive identifiers like social security number, driver's license number, or login credentials, CCPA defines consumers' "Personal Information" to include, among other things, IP address, device ID, cookie ID, browsing history or other online activity, purchasing history, geolocation data, biometric information, or any other information "that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

The statute imposes a number of new disclosure obligations on covered "Businesses." It also gives consumers (i.e., any California resident) significant new rights to request that a Business disclose what categories or specific pieces of Personal Information the Business has collected about them, and the third parties to whom the Business has "sold" or disclosed such information (the "Right to Know"); request that a business delete their Personal Information (the "Right to Delete"); and the right to direct a Business that "sells" Personal Information to stop selling their Personal Information (the "Right to Opt-Out"). (Businesses cannot sell the Personal Information of children without getting opt-in consent from children under 16 and the parents of children under 13.) Businesses must respond to valid requests and implement required deletion or opt-out within 45 days or less in most cases. Businesses are also prohibited from discriminating against consumers for exercising these rights.

There are potentially severe consequences for non-compliance. The California Attorney General has authority to bring civil enforcement actions against violators

and seek monetary penalties of up to $7,500 per violation. Consumers have the right to sue Businesses, individually or as a class, for breaches of their sensitive Personal Information, and can obtain statutory damages of up to $750 "per consumer, per incident," if the breach results from a Business's failure to maintain "reasonable security procedures and practices."

Here are six things companies should be doing or thinking about, if they aren't already:

1. **Is Your Company A Covered "Business" Under The CCPA?**

If you are a for-profit company doing business in California, and your annual revenues exceed $25 million, you are a Business.

If your annual revenues are less than $25 million, you are still a Business if you annually receive or share for commercial purposes the Personal Information of 50,000 or more consumers, households, or devices. If your website averages at least 4,167 unique visitors per month, this probably applies to you.

If your revenues are under $25 million, and you don't receive or share Personal Information on that scale, you are still a Business if you derive 50 percent or more of annual revenues from "selling" consumers' Personal Information.

Don't assume that your company isn't a Business just because its offerings are exclusively "B2B." The CCPA does not make such an exception.

2. **If You Think You Don't "Sell" Personal Information, Think Again.**

The CCPA threatens Businesses with the privacy equivalent of a Scarlett Letter: If you "sell" Personal Information, you must declare that in your privacy policy, post a prominent "Do Not Sell My Personal Information" button on your website, and stop "selling" a consumer's Personal Information if they submit a Request to Opt-Out. Forget your traditional notion of what a "sale" of data looks like. The CCPA defines "Sale" to include, among other things: "disclosing, disseminating, making available, transferring or otherwise communicating . . . a consumer's personal information by the business to another business or third party for monetary or other valuable consideration." As a practical matter, this means that if you share Personal Information with a third party, and as part of that relationship you receive a service or benefit that you are not otherwise entitled to, you may be Selling personal information.

All Businesses need to scrutinize their data flows carefully, starting with those relating to their digital advertising relationships and use of third party analytics or social media business tools. There may be Sales of Personal Information lurking in your use

of Facebook Business Tools, Google Analytics and Google advertising tools, "Like" buttons, or other such tools unless you start making changes now.

3. Turn Vendors Into "Service Providers."

If a Business wants to avoid branding itself as a Seller of consumers' Personal Information, the first step is for it to update its agreements with vendors that collect data on its behalf or with whom it shares data. Disclosure of Personal Information to a "Service Provider" is not a Sale, provided that your agreement explicitly prohibits them from Selling the Personal Information, prohibits them from using the Personal Information for any purpose other than the purpose set forth in your agreement, and contains other restrictions set forth in the CCPA. Google is offering a new setting called "restricted data processing" for its analytics and advertising tools that is supposed to help turn Google into a Service Provider, but activating that setting is no substitute for your own diligence. So far, Facebook's CCPA message to companies using its business tools appears to be: "You're on your own."

4. Consider Changing How Your Website Uses Browser Cookies And Similar Tracking Technologies.

Your website is almost certainly storing one or more "cookies" in the browser of each visitor to your website. Cookies, and the cookie IDs they typically hold, can be used to distinguish between visitors and track a visitor's online activity. If you allow advertisers, analytics providers, or social media partners to set their own "third party" cookies through your site, you may be sharing IP addresses, browsing activity, and other Personal Information about your site visitors with those third parties automatically after your site loads in the visitor's browser.

If you can't make those third parties your Service Providers, you may still be able to avoid Sales by making third party cookies and related sharing of Personal Information contingent on explicit, opt-in consent from the end user. That's because the CCPA specifies that a Sale does not occur when "[a] consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party." Consider deploying a pop-up cookie banner that requires some clear, affirmative act of direction or consent from the end user before some or all non-essential cookies, including third party cookies, can be stored in the user's browser. But bear in mind that "[h]overing over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party."

5. Update Your Privacy Policy and HR Privacy Notices.

Under the CCPA, a Business must post its privacy policy on its website, and the policy must now clearly and succinctly cover all online and offline collection of Personal Information. Among other things, the privacy policy must disclose what categories of

Personal Information a Business has collected, Sold, or disclosed for a business purpose during the past 12 months. If a Business doesn't Sell Personal Information, it must state that in the privacy policy. In addition, the policy must explain consumers' rights under the CCPA and provide mechanisms for exercising those rights, including web forms to submit Requests to Know, Requests to Delete, and (where applicable) Requests to Opt-Out.

Due to one of many recent amendments to the CCPA, a Business's California job applicants, employees, and other personnel don't have the right to make Requests to Know, Delete, or Opt-Out with respect to their Personal Information used strictly for employment or benefits reasons. But those individuals are still entitled to receive notice "at or before" the point of collection of the categories of Personal Information the Business collects about them and the purposes for which it is used. And they still have the right to sue for a breach of their sensitive Personal Information (such as their full name in combination with their social security number).

6. Compliance Is A Big Undertaking, And There's No Time To Wait.

The Attorney General has yet to finalize the CCPA's implementing regulations, and won't begin enforcement action until July 1, 2020. But the Attorney General has made clear that come January 1 he expects companies to be compliant, or to at least be making substantial progress towards compliance, and that uncured violations that take place during the first six months of 2020 may still result in penalties. If your company is a covered Business, updating your privacy policy is just a small fraction of what needs to be done. Most of the compliance work takes place in the form of mapping data flows to ensure disclosures are accurate and complete, carefully analyzing whether the Business Sells Personal Information, minimizing collection and retention of Personal Information, updating vendor agreements, and developing processes for receiving, verifying, responding to, and implementing consumer requests. It's time to get started if you haven't already.

Travis Brennan is a shareholder at Stradling and chairs the firm's Privacy & Data Security practice group, which has been advising financial institutions, retailers, software and app developers, geolocation providers, publishers, advertisers, IT service providers, and other clients on preparing for the CCPA since the law's enactment in 2018. The group includes regulatory specialists and trial lawyers with experience handling data incident response and defending companies in government investigations, consumer class actions, and commercial litigation arising from such incidents. Ahmad Takouche is an associate at the firm with experience in data privacy counseling and litigation.