BakerHostetler

Guidance

The California Consumer Privacy Act: Frequently Asked Questions

The California Consumer Privacy Act (CCPA) is a comprehensive new consumer protection law set to take effect on January 1, 2020. In the wake of the CCPA's passage, approximately 15 other states introduced their own CCPA-like privacy legislation, and similar proposals are being considered at the federal level. However, so far only Nevada has passed new consumer privacy laws, adding a "do not sell" right to its existing online privacy law, effective October 1, 2019.

Among the many differences between the CCPA and existing U.S. privacy legislation, the definition of personal information under the new law is very broad and includes data elements not previously considered personal information under any U.S. law. In addition, the CCPA introduces new privacy rights for Californians, such as the right to know what personal information a business has collected about them and the details on how the business uses and discloses the data, and the right to request that the business delete that information.

The CCPA will apply to a wide range of businesses that handle Californians' personal information, obligating them to comply with a host of new requirements governing their collection, use and sharing of personal information. Most will need to update the disclosures in their privacy notices, establish processes for responding to consumer rights requests, observe restrictions on data monetization practices and revisit relationships with vendors that handle personal information on their behalf.

The California legislative season ended on September 13 with the passage of six bills that will amend the CCPA if they are signed by the governor by October 13. Most notable among the amendments is a one-year delay in the law's coverage of human resources data and business-to-business communications. The first draft of proposed regulations interpreting and implementing the CCPA is expected by early October. Although some aspects of CCPA readiness should wait until those draft regulations have been released, there is much that can and should be done between now and then.

Below we address some of the questions clients frequently ask about the business impacts of the CCPA. Implementation challenges inevitably will arise as a company works to apply these new requirements to its business practices.

The time is now to start preparing for the CCPA, as well as for other new U.S. privacy laws that are likely to follow

Question: Does the CCPA apply to my business? What if we don't have operations in California?

Answer:

The CCPA will impact many businesses and business activities not previously subject to privacy regulations in the United States. The law is not limited in scope to entities that have physical operations in California; it applies to for-profit entities "doing business" in the state to which any of the following apply:

- Gross annual revenue is in excess of $25 million.
- Annually buy, receive for commercial purposes, sell or share for commercial purposes personal information of 50,000 or more California consumers, households or devices.
- Derive 50% or more of their annual revenues from selling California consumers' personal information.

The CCPA also applies to any entity that (1) controls, or is controlled by, a business that meets the above criteria, and (2) shares common branding with that business.

Question: Does the $25 million revenue threshold apply to California revenue specifically, or is it $25 million for the business as a whole?

Answer:

Unclear. Because the text of the law does not specify, the prevailing consensus seems to be that the threshold is $25 million overall, regardless of the total amount of revenue generated in California. This assumption seems validated by the fact that the other two prongs of the definition specify that they apply to California consumers. The same qualification could have been inserted in the first prong, but it was not.

Question: Will the CCPA be amended? What are the open issues?

Answer:

As we reported in early September 2018, the CCPA was already amended once – and the 2019 California legislature has now passed six additional amendment bills that the governor has until October 13 to sign or veto. The current version of the law contains certain typographical errors and unintentional mistakes that have been acknowledged on all sides, many of which would be corrected by the 2019 amendments. The most notable amendments are provisions that would delay for one year the application of most of the consumer rights provided by the CCPA to personal information that was collected from a consumer in connection with being a job applicant, employee or independent contractor, and to personal information that is part of certain business-to-business communications.

Question: What new rights will the CCPA give to California residents?

Answer:

The new rights under the CCPA are to some extent inspired by those of the EU's General Data Protection Regulation, so companies that have prepared to comply with data subject requests under that regime may be able to leverage their efforts when preparing to comply with the CCPA. The CCPA gives California residents the right to request that a business:

- Disclose the categories and specific pieces of personal information it has collected.

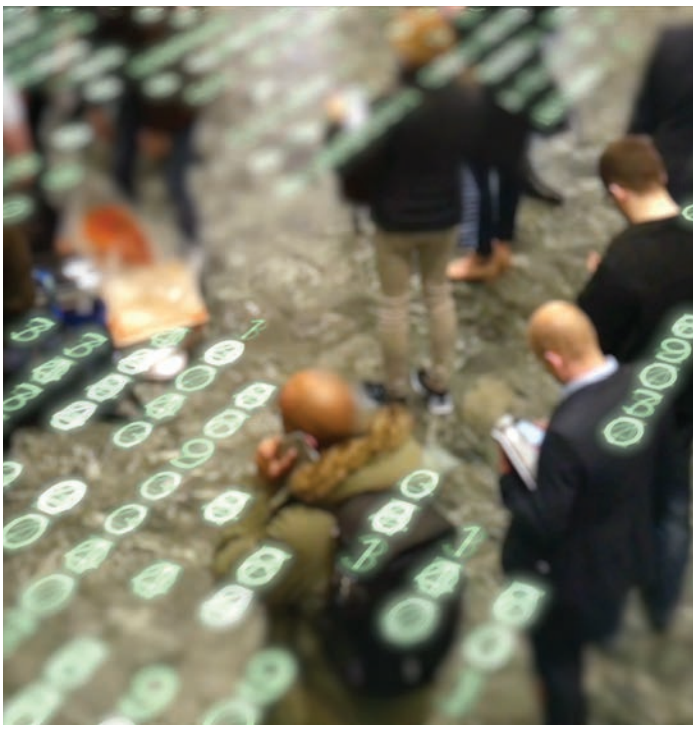
- Disclose the categories of sources from which the personal information is collected.
- Disclose the business or commercial purpose for collecting or selling the personal information.
- Disclose the categories of third parties with which the business shares the personal information.
- Delete any personal information about the consumer that the business has collected from a consumer, subject to certain exceptions.
- Not "sell" (broadly defined) the consumer's personal information (the "do not sell" opt-out).

Businesses typically must respond to requests that call for disclosure or delivery of personal data within 45 days of receipt, and must provide certain easily accessible, cost-free methods for consumers to exercise these rights. However, the timing for compliance with "do not sell" and deletion requests is less clear.

Question: Will we need to amend our company's online privacy policy?

Answer:

Yes, or at least provide a new form of California privacy notice. The CCPA has added several new substantive elements to the required disclosures that must be included in a privacy notice or policy. In addition to the information that must be included under the existing California statute or provided pursuant to California's



"Shine the Light" law, online privacy policies and any California-specific notice must include:

- A description of consumers' rights under the CCPA.
- A description of the categories of personal information collected by the business in the preceding 12 months.
- The commercial and business purposes for which the personal information is collected.
- The categories of personal information sold or disclosed for a business purpose in the preceding 12 months.
- The categories of third parties with which personal information is shared.
- A link to a "Do Not Sell My Personal Information" web-based opt-out tool.
- A description of any financial incentives for providing data or not exercising rights (e.g., if the company offers a 15% discount to individuals who provide their email address for marketing purposes, this incentive must be disclosed in the privacy policy).
- Two or more designated methods for submitting information requests, including a toll-free number and a website address (if applicable), though a pending amendment will not require a toll-free number for any purely online business.

Question: How do the "copycat" CCPA laws being proposed in other states compare with the CCPA?

Answer:

In 2019, 15 states proposed laws that are virtually identical to the CCPA with minor differences, or that are similar in certain ways but with key differences. As of September 16, 2019, only Nevada has passed new consumer

privacy legislation. The Nevada law, effective October 1, 2019, requires operators of online services to provide Nevada residents with the right to opt out of the sale of certain covered data collected via online services, but the definition of sale is far narrower than under the CCPA. Most other states' proposed laws have stalled, but a few, like that in Massachusetts (which would provide a broad private right of action for violations of the law), are still pending. North Dakota scaled back its proposal and passed a law requiring a study on what a potential privacy regulatory scheme should include. The prospect of businesses being required to comply with dozens of different state privacy laws has fueled interest in a federal law that would preempt state laws and provide a single set of compliance obligations.

We will continue to track and report on any significant legislative developments at the state and federal levels.

Question: How does a business confirm that a person making an access or deletion request under the CCPA is a California resident, or who they claim to be?

Answer:

Details regarding how to determine what constitutes a "verifiable consumer request" are to be included in the attorney general's regulations, which have yet to be promulgated. Ostensibly they should address who qualifies as a "California resident," and this issue has come up in the public forums with the attorney general's office regarding its development of the regulations. Regardless, a business could elect to accord CCPA rights to nonresidents, and in some cases this may facilitate compliance by eliminating the need to verify

California residency. That said, given the breadth of the definitions of personal information and sale, vexing questions remain regarding what a business must do, if anything, to tie pseudonymous data (e.g., online identifiers and browsing data) to a particular consumer seeking to exercise his or her rights.

Question: What should our company be focusing on right now, while we wait to see how these various state and federal law proposals shake out?

Answer:

While many businesses began CCPA preparedness in earnest last year, with uncertainty as the watchword, others started the year taking a "wait and see" approach to compliance. As the January 1, 2020, effective date nears, it is all but certain that there will be no federal law preempting CCPA, and businesses that have delayed CCPA preparations are now scrambling to come into compliance. While the regulations will likely not be final before the end of 2019, there is much that can be done in the meantime. For example:

- Companies should create a data inventory or data flow map to understand all the ways in which they may obtain personal information, the types of personal information they collect and share, the purposes for which they use it, the parties with which they share it and why, how it is retained and secured, and their current data disposal practices.

- With respect to disclosures, it is important to identify all the vendors and other third parties with which personal information is being shared and to review the existing contracts with those parties for compliance with existing and future laws. The CCPA includes complex rules regarding vendors and other recipients of personal information. Unless the attorney general's regulations narrow the definition of "sale," the ways in which data recipients are categorized will affect how a business is able to share the personal information of an individual who has submitted a "do not sell" request.
- It may be instructive to run a test internally to assess how prepared the company is to respond to a consumer request to access and/or delete their personal information. Ask yourself the following: Can your company verify the validity of the request? Find all the relevant personal information? Provide all the information the CCPA requires in a disclosure? Remove all the personal information from your systems, or establish a legal basis for retention? Honor a "do not sell" request?
- Ensure that the company has implemented sound and reasonable data security policies and procedures. The CCPA does not change California law in this regard, but it does drastically raise the stakes for security incidents by providing a private cause of action, with the possibility of statutory damages, for certain types of data breaches attributable to security inadequacies. While there will most likely be some delay in enforcement by the attorney general following January 1, 2020, the private right of action regarding security incidents becomes effective on the first of the year.

Question: What are the potential penalties for violations of the CCPA?

Answer:

Violations of the CCPA are subject to enforcement by the California attorney general's office, which can seek civil penalties of $2,500 for each violation or $7,500 for each intentional violation after notice and a 30-day opportunity to cure have been provided. Enforcement will be delayed until six months after publication of the final regulations implementing the CCPA, or July 1, 2020, whichever is sooner. The attorney general has been an outspoken critic of the CCPA's opportunity to cure provision, and the scope of that cure right is accordingly in question.

In addition, private plaintiffs may bring a civil action against a business in the event of a data security breach that results in unauthorized access and exfiltration, theft, or disclosure of the individual's personal information – if the breach is attributable to a failure to implement reasonable security procedures and practices appropriate to the nature of the personal information at issue. The statute allows for recovery of up to $750 per consumer, per incident, or actual damages, whichever is greater. That is thought to be the limit to the private right of action, and the very crux of the compromise between ballot initiative proponents and industry that led to the CCPA, but class action lawyers are expected to test this.

> Companies should create a data inventory or data flow map to understand all the ways in which they may obtain personal information, the types of personal information they collect and share, the purposes for which they use it, the parties with whom they share it and why, how it is retained and secured, and their current data disposal practices.

Question: Does my business qualify for one of the CCPA's exceptions?

Answer:

In addition to exceptions for compliance with the law – such as deidentified or aggregate consumer information, conduct occurring "wholly outside of California," and a few others – there are exceptions applicable to certain personal information already subject to state or federal regulation. These exceptions apply to types of information, not types of businesses or industries, so even companies that qualify for one of these exceptions will likely only be partially exempted. The excluded categories of personal information include (1) medical information or Protected Health Information governed by California law, HIPAA or the "Common Rule" applicable to clinical trials; (2) personal information subject to

the California Financial Information Privacy Act or the Gramm-Leach-Bliley Act (applicable to financial institutions); (3) personal information provided to or from consumer reporting agencies as governed by, and so long as maintained consistent with, the Fair Credit Reporting Act; and (4) personal information subject to protection under the Driver's Privacy Protection Act. One of the pending amendments would add exceptions for certain vehicle information disclosed for recall and warranty purposes.

Further, the CCPA includes exceptions where application of the statutory obligations would conflict with controlling state or federal law, such as the free speech protections of the First Amendment. As a result, the CCPA deletion right will not have the same reach as the EU's "right to be forgotten," at least with respect to publishers and other media. Companies also may be able to avail themselves of federal preemption in some instances. For example, the CCPA's prohibition on contract terms (such as arbitration clauses and class action waivers) that would limit consumers' CCPA rights arguably should be preempted by the Federal Arbitration Act. In addition, the CCPA expressly provides that a business is not required to act in a manner that could violate another consumer's rights.

In short, although your company may not have CCPA obligations with respect to some of the personal information it maintains – or not all of the CCPA's requirements will apply to that data – it is unlikely that a business otherwise subject to the CCPA will be wholly exempt by virtue of an exception under the law.

Conclusion

While it is likely that there will be additional refinements and clarifications of the CCPA through the regulatory rulemaking process, the fundamental requirements of the CCPA will not change further between now and the law's effective date. A new era of consumer privacy rights has dawned in the U.S., and businesses will need to have a sound understanding of the personal information they collect, process, use and share to be able to comply with the CCPA as well as any additional state or federal laws that may follow. As U.S. privacy law evolves in the coming months and years, the foundational work of building an information governance program will prepare your business to meet these developing challenges. For more information, see our U.S. Consumer Privacy and the CCPA page and follow our blog at dataprivacymonitor.com.

Contacts

Alan L. Friel
T +1.310.442.8860
afriel@bakerlaw.com

Laura E. Jehl
T +1 202.861.1588
ljehl@bakerlaw.com

Melinda L. McLellan
T +1.212.589.4679
mmclellan@bakerlaw.com

bakerlaw.com

Recognized as one of the top firms for client service, BakerHostetler is a leading national law firm that helps clients around the world address their most complex and critical business and regulatory issues. With five core national practice groups – Business, Intellectual Property, Labor and Employment, Litigation, and Tax – the firm has nearly 1000 lawyers located in 14 offices coast to coast. For more information, visit bakerlaw.com.

17.09.19.16.23_p05