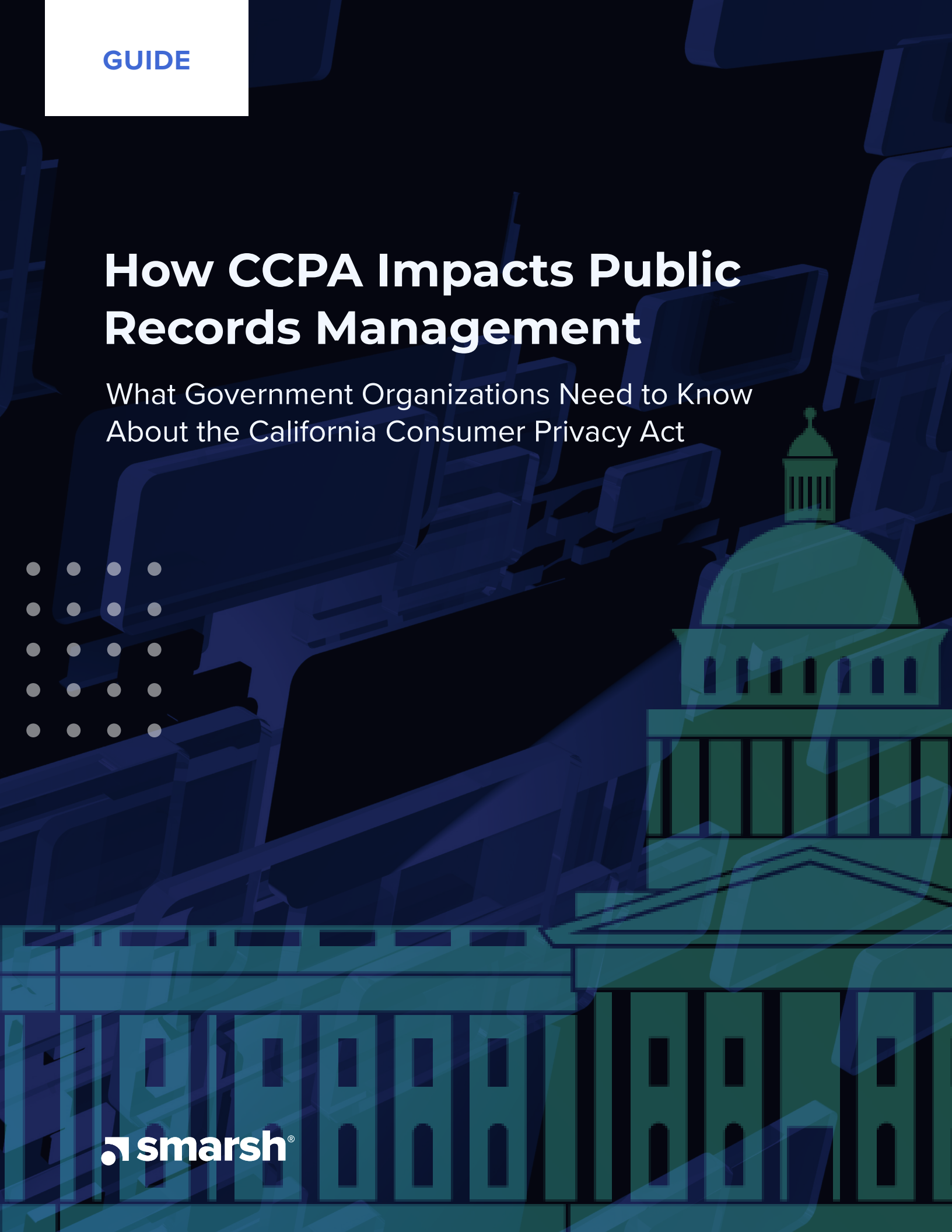
GUIDE

How CCPA Impacts Public Records Management

What Government Organizations Need to Know About the California Consumer Privacy Act



marsh®

What is the California Consumer Privacy Act?

The California Consumer Privacy Act (CCPA) established new consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses. It was enacted July 2018 and became enforceable July 1, 2020.[1]

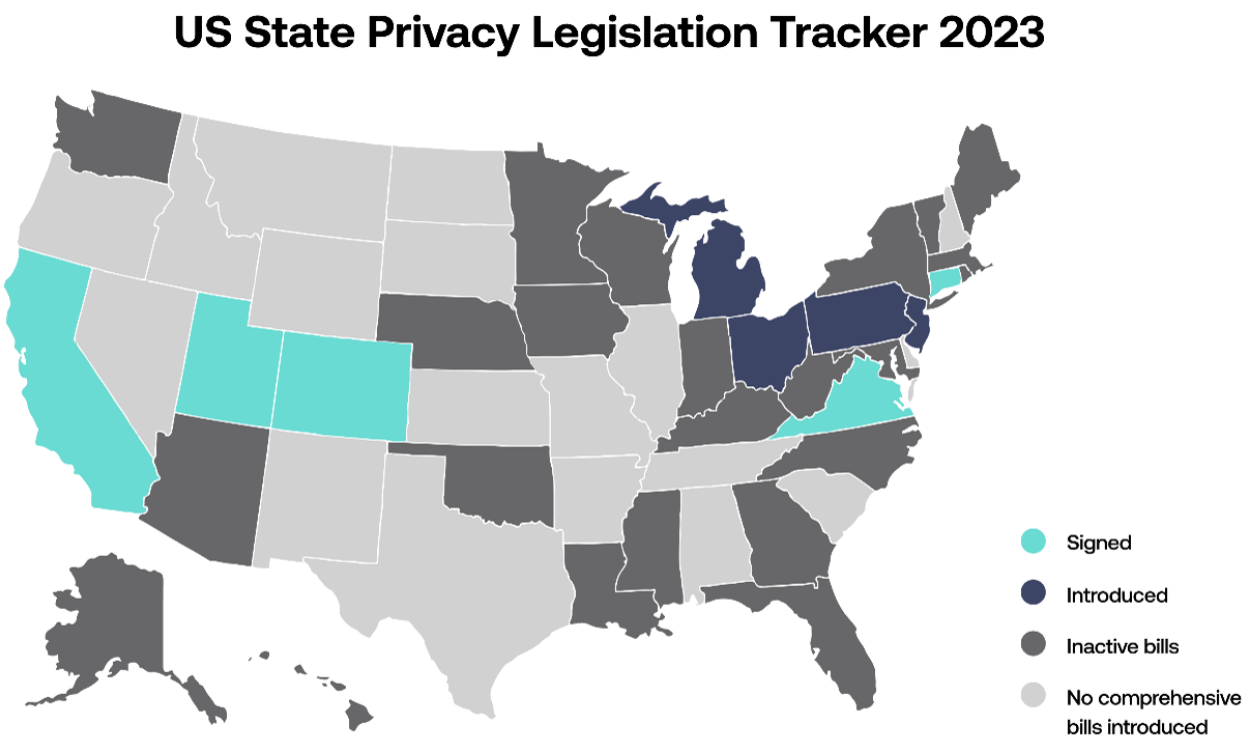
The CCPA allows California consumers to:

- Demand all information the company has collected and saved on them in the past 12 months
- Demand the deletion of their data
- Learn how their data is processed
- See a list of all third parties who may have access to their information
- Opt-out of the sale of their personal information to third parties
- Sue organizations if the privacy guidelines are violated, even if there is no breach

Organizations that must comply with CCPA are companies that:

- Conduct business in California (regardless of their home state or country)
- Collect consumer personal information
- Satisfy at least one of the following:
  - Have at least $25 million in annual revenue
  - Have personal data of at least 50,000 people
  - Earn more than half of their revenue from selling consumers' personal data

1 leginfo.legislature.ca.gov/faces/billTextClient



Source: iapp.org

What local governments can learn from CCPA

While CCPA does not currently apply to government organizations, many local government agencies — such as the Department of Motor Vehicles in some states — are already collecting, retaining and even selling potentially personally identifiable information (PII).

Public sector agencies should recognize that this data collection and use of personal data can put them in compromising positions should CCPA ever be expanded or if new data privacy laws are enacted.

What could the CCPA mean for organizations that must retain internal communications for record requests? Could workers require employers to delete their communications for privacy purposes? If employees request that communications they sent be erased under individual rights of the CCPA, would the organization have the means to search an archive and expunge those emails or text messages?

The answers to these questions are not yet clear, providing all the more reason for agencies to prepare for the evolving data privacy laws and their looming extension into state and local governments.

Here are five simple steps government agencies can learn from CCPA to get ahead of changing laws and strengthen data security:

1 Understand the data

Given the growing complexity and variety of communications and collaborative data, agencies should establish a good foundation in exploring how privacy controls (whether defined by policy alone or in combination with enforcement and technology) can be implemented or strengthened.

2 Update policies to reflect all sources used for business purposes

Ensuring consent and communication policies are current and reflect how personal data should be managed is central to any privacy mandate.

3 Identify the intersection of public records management with CCPA requirements

Provide workers and data managers with an overview of CCPA requirements and explore how public records management policies can align with the law.

4 Tune oversight processes to reflect high risk areas

Ongoing inspection of content for personal information shouldn't only focus on IT-controlled systems, but also those where rules and oversight have yet to be extended, such as public portals.

5 Use AI/surveillance to uncover dark data locations

Data privacy is a terrific use case for advanced analytics and surveillance technology to extend oversight processes into areas that cannot be uncovered by policies.

Conclusion

A major and consistent criticism of the CCPA since its enactment has been its exclusion of California state and local governments' collection and use of personal information. While the CCPA has not been updated yet to include agencies, it doesn't mean they are off the hook. There's been a great deal of momentum behind discussions on applying similar controls to California governments. And with the strong support and enforcement from the Californian government around data privacy — including building a privacy police force[2] — it proves that these laws are constantly evolving and can shift at a moment's notice.

2 www.nytimes.com/technology/california-privacy-agency-ccpa

Additional information about exemptions and penalty rules pursuant to the CCPA:

Exemptions listed under rule 1798.105 (d):

A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

- Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity
- Debug to identify and repair errors that impair existing intended functionality
- Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law
- Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent
- To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business
- Comply with a legal obligation
- Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information

Penalty listed under rule (1798.155)

Violations of the CCPA are enforceable by the California Attorney General, which is authorized to pursue civil penalties of up to $7,500 per violation.

smarsh®

Smarsh® enables companies to transform oversight into foresight by surfacing business-critical signals from the most in-demand communications channels. Regulated agencies of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisers and U.S. federal, state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com

Guide - 09/23

1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh