FROM CCPA TO CPRA

WHY YOU SHOULD TRACK CALIFORNIA'S PRIVACY LAWS

PREPARED BY

Beth Burgin Waller
Chair, Cybersecurity &
Data Privacy Practice

John Pilch
Cybersecurity/Privacy Analyst

April 22, 2021

WOODS ROGERS
ATTORNEYS AT LAW

woodsrogers.com

CONTENTS

INTRODUCTION

The data privacy laws coming out of California in early 2021 set new privacy standards that are useful to review regardless of your geographic location. Keep in mind if you are based outside California, but have employees or customers located there, these updates are of paramount importance to your business.

EXPERTS EXPECT THIS LAW TO PUSH MORE STATES AND EVEN THE FEDERAL GOVERNMENT TO PASS THEIR OWN DATA PRIVACY REGULATIONS.

Share of US companies working to comply with 2 or more privacy laws

79%

10% report working to comply with 50+ privacy laws

13% are working with 6-10 laws

13% with 11-49 laws

* "New IAPP and TrustArc Report Reveals a Majority of Companies Are Embracing a Single Global Data Protection Strategy," TrustArc, retrieved 2/3/2021, https://trustarc.com/new-iapp-and-trustarc-report-reveals-a-majority-of-companies-are-embracing-a-single-global-data-protection-strategy/

LEGISLATION

Californians voted to approve Proposition 24, the California Privacy Rights Act (CPRA), in November 2020. The legislation amended the California Consumer Privacy Act (CCPA) to expand the privacy rights of California residents significantly. The CPRA adds several elements similar to those in the European Union's General Data Protection Regulation (GDPR), currently considered the gold standard of privacy and data protection law.

CPRA also makes it almost impossible to weaken privacy protections in California in the future. CPRA gives the California Legislature the power to amend the law via a simple majority, but any amendment would have to be "in furtherance of the purpose and intent" of CPRA, which is to enhance consumer privacy. We anticipate the new rules in the CPRA will be around for a long time.

THIS REPORT REVIEWS THE MOST IMPORTANT CHANGES MADE BY THE CPRA.

These changes will take place according to the timeline on the following page.

TIMELINE

1

December 16, 2020

California Privacy Protection Agency Established and Funded

It will have a budget of $5 million for 2021 and $10 million each year thereafter.

2

March 16, 2021

Board Appointed

The five-member board, consisting of experts in privacy, technology, and consumer rights, was appointed.

3

July 1, 2021

Rulemaking Could Begin

The OAG will continue its existing rulemaking process until the Agency is prepared to begin rulemaking as soon as July 1, 2021.

4

July 1, 2022

Final Regulations Adopted

The Agency will adopt final regulations required by the CPRA no later than July 1, 2022.

5

January 1, 2023

Obligations Activated

Obligations for businesses under the CPRA and related regulations become active on January 1, 2023. Obligations will apply to personal information collected by a business on or after January 1, 2022.

This means the obligations take effect before the regulations are finalized, but most obligations will be clear well before January 1, 2022.

6

July 1, 2023

Enforcement Begins

Enforcement will begin July 1, 2023, and will only apply to violations occurring on or after that date.

THE REGULATOR

The California Office of the Attorney General (OAG) currently enforces the CCPA. The CPRA establishes a new entity, the California Privacy Protection Agency ("the Agency") and grants it the investigative, enforcement, and rulemaking powers presently held by the OAG.

Notably, there will be no gap between CCPA and CPRA enforcement. CPRA states enforcement of CCPA provisions will continue "and shall be enforceable until the same provisions of [the CPRA] become enforceable."

What are my next steps?

1. **There is time to get ready, but little time to waste.** Many companies preparing for GDPR waited until the six months before it took effect in May 2019, to start their program and then found it difficult to develop internal resources and obtain external advice and support. You know enough about the requirements today to get started on the CPRA. July 1, 2023, will be here sooner than you think.
2. **Real enforcement will happen.** Based on the current budget, the Agency could have nearly as many full-time privacy agents for California as the Federal Trade Commission (FTC)—the primary enforcer of privacy rules at the federal level has for the entire United States. Don't count on your industry or relative size to protect you from scrutiny.

PRINCIPLES

THE CPRA ADOPTS SEVERAL PRINCIPLES SIMILAR TO THOSE IN GDPR.

- **Data minimization**
  A business's collection, use, retention, and sharing of personal information must be minimized to what is reasonably necessary and proportionate to achieve the purpose of collection or processing, or for another disclosed purpose that is compatible with the context of collection. The personal information must not be subject to processing for incompatible, undisclosed purposes.
- **Purpose limitation**
  Businesses must not collect or use personal information for a new purpose that is incompatible with previously disclosed purposes without first providing notice to the consumer.
- **Storage limitation**
  Businesses must disclose, at the time of collection, their retention periods for each category of personal information (or if that is not possible, the criteria used to determine such period). Businesses are further prohibited from retaining personal information for longer than is "reasonably necessary" for each disclosed purpose.

What are my next steps?

1. **It is necessary to understand and document the categories of personal information your company collects and the reasons you collect it.** This will take time, and is one of the actions you could start immediately.
2. **You must ensure personal information collected for one purpose is not used for a different purpose.** This will have a substantial impact on the marketing and sales operations of some companies.
3. **You will need to dispose of some data.** It will take time to check your record retention policy, confirm the retention periods, locate all of the stale data, and delete it. You will need to consider both electronic and paper records. You could start this process immediately.

RIGHTS OF CALIFORNIA CONSUMERS

THE CPRA ADDS SEVERAL NEW RIGHTS & MODIFIES SOME EXISTING RIGHTS.

THE NEW RIGHTS ARE:

- **Right to Correction**
  Consumers may request correction of their personal information if that information is inaccurate.

- **Right to Restrict Sensitive Personal Information**
  Consumers may limit the use and disclosure of this data for certain secondary purposes, including disclosure to third parties, subject to certain exemptions.

- **Right to Opt Out of Automated Decision-Making Technology**
  CPRA directs the Agency to issue regulations governing opt-out rights, implying consumers may require human decision-makers in cases related to work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

- **Right to Access Information About Automated Decision Making**
  CPRA directs the Agency to issue regulations governing requests for meaningful information about the logic involved in a decision making processes and a description of the likely outcome based on that process, implying consumers have this right under CPRA.

THE MODIFIED RIGHTS ARE:

- **Right to Delete**
  When requested by the consumer, businesses are now required to notify third parties to delete any of the consumer's personal information bought or received.

- **Right to Know**
  The response to a "Right to Know" request is expanded to include personal information collected beyond the prior 12 months, if collected after January 1, 2022.

- **Right to Opt Out**
  In addition to the existing right to opt out of the sale of personal information to third parties, consumers can opt out of the "sharing" of personal information for cross-context behavioral advertising.

- **Opt-In Rights for Minors**
  The opt-in right now explicitly includes the sharing of personal information for behavioral advertising purposes. Also, businesses must wait 12 months before asking a minor for consent to sell or share his or her personal information after the minor has declined to provide it.

- **Right to Data Portability**
  Consumers may now request the business transmit specific pieces of personal information to another entity, to the extent it is technically feasible for the business to provide the data in a structured, commonly used, and machine-readable format.

What are my next steps?

1. **You should develop a clear process for handling each type of request.** A common, centralized process may work for some businesses, while others may find several separate processes more appealing. Some of the processes may be easier to automate or partially automate than others.

2. **It is necessary to understand and document all automated decision-making processes that affect consumers.** Will you be able to explain the algorithms clearly and concisely, without exposing trade secrets?

NEW & AMENDED DEFINITIONS

COVERED ENTITIES

The definition of a "business" is changed as listed:

- Increases the number of consumers or households from 50,000 to 100,000 while removing "devices" from the definition. This change will reduce applicability of the law to small and midsize businesses
- Expands applicability to businesses that generate most of their revenue from sharing personal information, not just selling it
- Extends the definition to joint ventures or partnerships composed of businesses that each have at least a 40% interest
- No change to the minimum annual revenue of $25 million (organizations with revenues lower than this are not covered by CCPA and CPRA)
- No change with regard to non-profits, which are not covered in either law

What are my next steps?

Does CPRA actually apply to you? Before taking any further steps, evaluate your company according to the new definition.

SENSITIVE PERSONAL INFORMATION

This category of data is subject to new disclosure requirements, and consumers have new rights designed to limit businesses' use of their sensitive personal information.

Sensitive Personal Information includes:

- Government identifiers (such as Social Security numbers and driver's license numbers)
- Financial account and login information (such as credit or debit card number together with login credentials)
- Precise geolocation
- Race, ethnicity, religious or philosophical beliefs, or union membership
- Content of nonpublic communications (mail, email, and text messages)
- Genetic data
- Biometric or health information
- Sex life or sexual orientation information

The CPRA definition of "Sensitive Personal Information" is broader than the GDPR definition, which does not include content of nonpublic communications, government identifiers, and financial account and login information.

On the other hand, CPRA recognizes and treats differently the incidental collection of sensitive personal information. An example is a photograph of a person, which could reveal race, ethnicity, or religious beliefs even if that were not the photograph's purpose. According to CPRA, "sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer … shall be treated as personal information." GDPR does not recognize the difference.

What are my next steps?

1. **It is necessary to understand and document the sensitive personal information your company collects.** This will take time and is one of the actions you could start immediately.
2. **Companies already subject to GDPR must take care in this area.** It is one of the few in which CPRA is broader than GDPR.

MARKETING & ADVERTISING

First, CPRA resolves uncertainty related to the meaning of the word "sell" by defining the word "share" and adding it to nearly all requirements using the word "sell." Several well-known companies have used the existing ambiguity to claim they are not selling data. This will be much more difficult under CPRA.

Second, CPRA distinguishes between two types of advertising, defined as follows:

1. **Cross-context behavioral advertising**
   The targeting of advertising to a consumer based on personal information obtained from activity across businesses, branded websites, applications, or services, other than those with which the consumer intentionally interacts. Note that "hovering over, muting, pausing, or closing a given piece of content does not constitute" intentional interaction.

2. **Non-personalized advertising**
   Advertising and marketing based solely on a consumer's current interaction with the business and the personal information derived from it.

The sharing of personal information for cross-context behavioral advertising is subject to the right to opt out.

The use of personal information for non-personalized advertising is not subject to opt out. It is instead designated as an internal "business purpose."

These definitions and the related requirements are an attempt to regulate digital advertising and they solidify a current interpretation of the CCPA.

Finally, CPRA states it does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs. There was some confusion in this area previously.

What are my next steps?

Businesses need to evaluate their processes using the new definitions. The addition of the word "share" closes a substantial loophole which may require businesses to change their operations or even their business model.

CONSENT

The CPRA provided a definition of consent that is close to the strict standard used in Europe. The concept of consent is used in a few scenarios, some of which already required consent under the CCPA:

- Consenting to the sale or sharing of personal information after an opt-out
- Minor opt-in consent for sale and sharing of personal information
- Consenting to secondary use and disclosure of sensitive personal information after an opt-out
- Exemptions for research
- Opt-in consent for financial incentive programs

What are my next steps?

It is necessary to review the definition of consent and ensure that any consent collected meets the CPRA definition. Businesses will need to develop a way to document consent. Since regulations clarify the requirements and the number of scenarios is small, some businesses may wait to address this aspect of CPRA.

OTHER PARTIES

The CPRA amends the definition of "service provider" and introduces "contractors," a new category of recipients of personal information who process the personal information made available to them pursuant to a written contract. Contracts with both service providers and contractors must now:

- Specify that information is provided for limited and specified purposes
- Obligate the person receiving information to comply with the CPRA and "provide the same level of privacy protection as is required by" the CPRA
- Grant the business the right to ensure information is being transferred "in a manner consistent with the business's obligations under this title"
- Require the person receiving the personal information to notify the business if it can no longer meet the obligations of the CPRA
- Grant the business the right to take steps to stop and remediate unauthorized use of personal information
- Require contractors to certify they understand and will comply with such contractual obligations

Most importantly, CPRA makes each company responsible for what their service providers and contractors do with the personal information they are sold or provided.

What are my next steps?

1. **Businesses must understand and document their personal information "ecosystem."**
   - Which service providers and contractors receive personal information from us?
   - Do those service providers and contractors pass the personal information down to a second level of service providers and contractors? How deep does it go?
   - This planning phase will take time, and is one of the actions you could start immediately.
2. **Companies must modify their terms and conditions in contracts involving personal information. The** Agency may specify standard clauses, or common wording may develop on its own, so it is reasonable to wait to begin the implementation phase.

EXEMPTIONS

EMPLOYEE & BUSINESS-TO-BUSINESS EXEMPTION

The CPRA extends the employee and business-to-business (B2B) exemption to January 1, 2023, allowing two years for the California Legislature to address employee and B2B privacy questions in a separate bill.

The CPRA states its intent to treat employee and B2B personal information differently than consumer personal information. It is difficult to predict what the California Legislature will do, and this approach is different from that taken in Europe by GDPR.

What are my next steps?

The best approach to these items is to wait for more clarity from the Agency.

CONTROLS

CPRA requires businesses to "implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure." This is similar to the GDPR requirement of "appropriate technical and organizational measures." Like GDPR, CPRA does not provide a list of specific controls, as the pace of technological change quickly makes such lists out-of-date. The general categories, include such items as:

- Security Governance
- Logical access control
- Physical access control
- Employee vetting and training
- Vendor security
- Network security
- Endpoint security
- Backup and recovery procedures
- Configuration management
- Vulnerability and patch management

What are my next steps?

1. **It is not too soon to start identifying and documenting controls.** Many will be in place already, either to comply with other regulations (SOX, PCI DSS, HIPAA, GLBA, etc.) or to protect the company regardless of regulations.
2. **It is important to keep in mind both the data properties and the data types protected.** For example, SOX controls protect the integrity of financial data and financial reporting. Controls for CPRA protect integrity, confidentiality, and availability of personal information. Make sure the combination of controls applied actually achieves the goal.

The Agency is likely to provide additional guidance before CPRA becomes enforceable.

RISK ASSESSMENTS & AUDITS

CPRA identified this area as one requiring further regulations, but offers the following thoughts:

- **Risk Assessment**
  Companies should submit a risk assessment to the Agency on a regular basis.

  The document should describe their processing of personal information, including sensitive personal information (if applicable). The assessment also should identify and weigh the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with such processing.

  The goal would be to restrict or prohibit such processing if the risks to privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public.

- **Agency Audit**
  The Agency is required to "appoint a Chief Auditor to conduct audits of businesses to ensure compliance." Further regulations will be needed to establish criteria for selection of audit targets and to define the scope and process for conducting the audits.

- **Cybersecurity Audit**
  Companies should have a thorough and independent audit of their cybersecurity protections every year.

What are my next steps?

The best use of your time is to wait for the final regulations. Depending on the final regulations, the cybersecurity audit could be large enough to affect the budget of the IT/Cybersecurity/Audit/Privacy organization, so it is helpful to keep an eye on the regulations and plan accordingly.

CONCLUSION

California's existing privacy regulation is merely a first step into murky privacy waters. The new CPRA goes much further by refining definitions, sharpening requirements, and expanding oversight.

The CPRA will be fully enforced by January 2023, whether your business is ready or not. All affected businesses must work towards compliance immediately.

CONTRIBUTORS

BETH BURGIN WALLER

Chair, Cybersecurity & Data Privacy Practice

(804) 343-5039 or (540) 983-7625
bwaller@woodsrogers.com

Certified Information Privacy Professional with U.S. and Europe designations (CIPP/US & CIPP/E)
Certified Information Privacy Manager (CIPM)

Beth advises clients both on cybersecurity concerns and privacy regulatory compliance. Her experience on the intersection of technology and the law is extensive. Her clients range from Fortune 200 companies to municipalities to universities and span diverse industry sectors.

JOHN PILCH

Cybersecurity/Privacy Analyst

(804) 343-5021
jpilch@woodsrogers.com

Certified Information Systems Security Professional (CISSP)
Certified Information Privacy Professional with U.S. and Europe designations (CIPP/US & CIPP/E)

John brings more than 20 years of experience in global privacy and data protection and internal control and finance at two Fortune 500 companies. John has specific expertise in identifying risks, applying control frameworks (NIST, COSO, ITIL, COBIT), and developing and implementing corrective actions.

WOODS ROGERS
ATTORNEYS AT LAW

(800) 552-4529

woodsrogers.com