The California Privacy Rights Act: What it is, Why it is Significant, and How to Prepare

Scott M. Giordano, Esq., FIP, CISSP  
V.P. and Sr. Counsel, Privacy and Compliance

K Royal, FIP, CIPP/E / US, CIPM, CDPSE  
Associate General Counsel, TrustArc

July 21, 2020
Presenters

Scott Giordano, Esq., FIP, CISSP
VP and Sr. Counsel, Privacy and Compliance, Spirion
- Specializing in multinational/cross-border aspects of data protection
- ISO 17024 Certifications Advisory Board Member, International Association of Privacy Professionals
- Created and taught the first law school course on electronic evidence and -discovery
- Member of the California, the District of Columbia, and Washington state bar associations

K Royal, FIP, CIPP/E / US, CIPM, CDPSE
Associate General Counsel, TrustArc
- Former RN turned attorney, focused on privacy, tech, and life sciences
- Active in leadership for professional associations, such as IAPP and ACC
- Featured tech / privacy columnist for Association of Corporate Counsel
- Adjunct professor at Sandra Day O’Connor College of Law at ASU
- Co-host of the Serious Privacy podcast [https://trustarc.com/resources/serious-privacy-podcast/](https://trustarc.com/resources/serious-privacy-podcast/)
If you leave with nothing else…

• If the CPRA wins at the ballot box, it will be set in stone.
• Makes major changes to key privacy definitions, creates a new class of personal information, and creates a new government agency to enforce it.
• Understanding what qualifies as personal information (and special personal information), where it lies in your business, and who has access to it is key – especially third parties like licensees and cloud service providers.
Summary of the Proposed Initiative

Official title: *California Privacy Rights Act of 2020 (CPRA)*. Ballot initiative can be found here:


- If passed by the voters, applies to information collected on or after January 1, 2022; the Act will go into effect January 1, 2023.

- Currently, voter support is highest for any initiative in California history
Principle Changes

- Creation of the **California Privacy Protection Agency (CPPA)**, tasked with enforcement of the CPRA and other state privacy regulations. In GDPR terms, a Supervisory Authority.
- Performs “administrative” enforcement:
  - “The Agency may subpoena witnesses, compel their attendance and testimony, administer oaths and affirmations, take evidence and require by subpoena the production of any books, papers, records or other items[.]”
- A “Chief Privacy Auditor” will be appointed to conduct audits of businesses.
- Grants a statute of limitations for the Agency to enforce the CCPA for five years.
- Civil enforcement still performed by the A.G.
Principle Changes

Introduces the concept of “sensitive personal information,” defined as:
• Social Security number
• Driver’s license number
• State identification card number
• Passport number
• A consumer’s account log-in, financial account, or debit card or credit card number in combination with any required security or access code, password or credentials allowing access to an account;
• A consumer’s precise geolocation;
• Personal information revealing a consumer’s racial or ethnic origin, religion, or union membership;
• The contents of a consumer’s private communications, unless the business is the intended recipient of the communication;
• A consumer’s biometric information;
• Data concerning a consumer’s health;
• Data concerning a consumer’s sexual orientation;
• or other data collected and analyzed for the purpose of identifying such information
Principle Changes

- Enables consumers to direct businesses not to use or disclose their SPI (i.e., opt out; presumably, another opt-out button would be needed on a website).
- Consumers must opt in for sale of their SPI.
- Can not be used for cross-context behavioral advertising.
Principle Changes

• Introduces the concept of “cross-context behavioral advertising.”
• Defined as the “targeting of advertising to a consumer based on a profile of the consumer, including predictions derived from the consumer’s personal information, where such profile is related to the consumer’s activity over time and across time and multiple businesses or across multiple, distinctively branded websites, applications, or services.”
• “Sale” now includes disclosure of cross-context behavioral advertising
• Upshot: All the rules re: sales apply, including right to opt out
• Also, cross-context behavioral advertising is not considered a “business purpose,” meaning that such information can no longer be used internally
Principle Changes

• Introduces the concept of “non-personalized advertising”
• Defined as “advertising and marketing that is not based on a consumer's past behavior.”
• Relevant because it doesn’t fall under the rules governing sales or business purposes
Principle Changes

**Information security.**
- Creates “large data processors,” businesses that collect more than 5 million consumers’ personal information annually
- Required to conduct cybersecurity audits and publish risk assessments pursuant to regulations **to be issued** by the Agency.
- New positive mandate: “A business that collects a consumer’s personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access.”
- Also note re: “curing” a breach: “The implementation and maintenance of reasonable security procedures and practices following a breach does not constitute a cure.”
- *Remember the expanded definition of personal information.*
Other Changes

Personal information.

“Personal information” is defined as “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.”

“Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household[.]”
Other Changes

Minors.
• Prohibits businesses from collecting the personal information of children under 16 unless the child (if 13 or older) or parent has affirmatively consented to the collection (i.e., opted in)
• Under today’s CCPA, just the sale is limited, not the collection, of personal information from minors.
• Penalties for any violations of the CCPA involving minors’ personal information would be tripled to $7,500.
Other Changes

Access and correction.
Consumers have a right to correct inaccurate personal information.
Other Changes

Amends the definition of a “business” to include any for-profit entity that collects consumers’ personal information, determines the “purposes and means” of the processing of that information, conducts business in CA, and meets one or more of the following:

(A) has annual gross revenues greater than $25,000,000 in the preceding calendar year; or

(B) alone or in combination, annually buys or sells the personal information of 100,000 or more consumers or households; or

(C) derives 50 percent or more of its annual revenues from selling consumers’ personal information.
Other Changes

Households
(Finally) defines a “household” as “a group, however identified, of consumers who cohabitate with one another at the same residential address and share access to common device(s) or service(s) provided by a business.”
Other Changes

“Deidentified” data.
Amends the definition of “deidentified” to “information that cannot reasonably be used to infer information about, or otherwise be linked to, an identifiable consumer,” if the business takes reasonable measures to prevent that linking and mandates third parties to adhere to this CCPA section.
Currently:
(h) “Deidentified” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information[.]
Other Changes

• **Employee data and business-to-business due diligence.**
• Makes the limited employee-data and business-to-business exemptions permanent, instead of sunsetting after one year, which is the case now.
• Not surprising, given that employees weren’t contemplated by the original CCPA drafters.
Other Changes

• **Right to access personal information – time limit**
• Does away with the rolling 12-month limit unless “unduly burdensome.”
• Essentially like GDPR.
Other Changes

“Publicly available” information

“[P]ublicly available” means information that is lawfully made available from federal, state, or local government records or information that a business has a reasonable basis to believe is lawfully made available to the general public from widely distributed media, or by the consumer, or by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. “
Other Changes

Data minimization.

• “A business’s collection of a consumer’s personal information shall be limited to personal information that is reasonably necessary to achieve the purposes for which it is collected.”

• Compare to the GDPR Art. 25:
• “The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.”
Other Changes

Data quality.
“A business that collects a consumer’s personal information shall take reasonable steps in light of the nature of the personal information and the purposes of processing the personal information to ensure that it does not collect, retain, or share inaccurate personal information.”
Other Changes

Contractors.
Under existing CCPA:

w) “Third party” means a person who is not any of the following:

• The business that collects personal information from consumers under this title.

• A person to whom the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract [prevents use, sale, etc. of the personal information involved].

• In other words, a contractor!
Other Changes

Contractors.

• Under CCPA 2.0:
• (j) (1) “Contractor” means a person to whom the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract:
  • (A) Prohibits the contractor from [use, sale, etc. of the personal information involved].
  • (B) Includes a certification made by contractor that the contractor understands the restrictions in subparagraph (A) and will comply with them.
## Getting Ready

<table>
<thead>
<tr>
<th>Process Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nerve Center' Country (dropdown)</td>
</tr>
<tr>
<td><strong>Country</strong></td>
</tr>
<tr>
<td>United States</td>
</tr>
<tr>
<td>United States</td>
</tr>
</tbody>
</table>

Reproduced with permission from Robert Half Legal Consulting
How To Get There From Here

Create your data inventory – there’s more than you think

Create your DSAR process – data subject access request
• Includes verifying the requestor

Determine what you’re going to put into the report and how you’re going to package it into a reasonably useable form

Determine delivery mechanism:
• Customer account
• Email
• Snail mail

Have a protocol to make sure that nothing falls through the cracks

Prepare draft updates to your privacy statement
Summary and Conclusions

• Even more demanding than CCPA 1.0
• Not unlike the GDPR and will involve Legal, Marketing, HR, Product Management, and others
• More guidance will be needed in several areas. Lots more.
• Penalties will be severe
• Get started now with your data inventory
• The legislature can’t come to the rescue
Thank you!
Scott M. Giordano, Esq.
Scott.Giordano@Spirion.com

K Royal
KRoyal@trustarc.com

Learn more about how Spirion can help accelerate CCPA compliance through automated accurate data discovery, classification and monitoring.

Visit www.spirion.com

All trademarks are the property of their rightful owners.