Association of Test Publishers' Security Committee (ATPSC)
PRIVACY IN PRACTICE BULLETIN
A Publication of the ATPSC International Privacy Subcommittee

Bulletin 18
January 8, 2024

The California Privacy Rights Act and Finalized Regulations[1]

Summary of key updates:

- The California Privacy Rights Act ("CPRA") is in force and amends the California Consumer Privacy Act ("CCPA"); the updated California Consumer Privacy Act Regulations ("CCPA Regs") are enforceable from March 29, 2024, except for several proposed regulations, *including on* the *use of automated decision-making*, that have not yet been adopted (and which will become effective one-year after promulgation);
- A new administrative agency, the California Privacy Protection Agency ("Agency"), has been created and shares enforcement authority with the California Attorney General ("Cal AG");
- Exemptions in the CCPA for employment and business contact personal information have expired and the CPRA applies to these categories of personal data;
- In addition to other new rights introduced by the CPRA, consumers now have the right to opt-out of "sharing" as well as the "sale" of personal information. Businesses engaged in such activities must recognize such rights and provide a website opt-out link, as well as comply with global privacy controls requirements;
- Contracts with vendors should be updated to include prescribed language so that where appropriate these organizations are treated as "service providers" under the CPRA;
- There is now no automatic right to cure a CCPA violation and the possible fines per violation have been substantially increased, especially for misuse of children's personal information and intentional violations;
- Published enforcement examples may indicate current enforcement priorities in the areas of advertising technology, failure to honor opt-out rights, and non-compliant notices.

INTRODUCTION

This Bulletin provides a current update on California privacy, following the CPRA going into effect and other recent developments. The ATPSC International Privacy Subcommittee has published two prior bulletins on California privacy laws/regulations: Bulletin 6 (December, 2019) and Bulletin 12 (January, 2021). Readers are encouraged to review those bulletins prior to reading this bulletin.

Following developments in California privacy is challenging. A brief timeline is provided below to assist users in tracking regulatory developments.[2] The CPRA became effective less than three years after enforcement of the CCPA began, introducing new and revised obligations. The CCPA Regs, which have

[1] ATP acknowledges contributions by Jamie Armstrong, Gary Behrens, Melissa DeWees, and Donna McPartland.
[2] It is important to note that, in some cases, information in Bulletins 6 and 12 is superseded by recent developments. For example, Bulletin 12 was published in January, 2021, after certain modifications were made to the original CCPA Regs but prior to later amendments that did not go into effect until March 2021.

an important role in explaining how to comply with the law, have been amended several times. Testing organizations now have to familiarize themselves with further updated CCPA Regs, made to harmonize them with the CPRA amendments to the CCPA and operationalize new rights and concepts introduced by the CPRA.[3]

As of the date of this Bulletin, covered testing organizations should be familiar with both the CCPA as amended by the CPRA[4] and the updated CCPA Regs.[5] **It also should be noted that the updated CCPA Regs finalized by the Agency are not enforceable until March 29, 2024** and therefore requirements contained in those regulations that are covered in this Bulletin will not formally apply until that date.[6] There are still other proposed regulations stemming from the CPRA that have not yet been finalized and adopted by the Agency; those regulations will go into effect one year after they are adopted.

TIMELINE

January 1, 2020:	CCPA in effect;
July 1, 2020:	CCPA enforcement by the Cal AG begins;
August 14, 2020:	Original CCPA Regs go into effect;
October/December 2020:	Cal AG publishes two further sets of modifications to the CCPA Regs;[7]
March 15, 2021:	Additional amendments to the CCPA Regs in effect;
January 1, 2023:	CPRA in effect;
March 29, 2023:	Original Agency-updated CCPA Regs effective date;
June 30, 2023:	California Superior Court postpones updated CCPA Regs enforcement;[8]
March 29, 2024:	Enforcement of Agency-updated CCPA Regs begins.

SUMMARY OF KEY UPDATES

---

[3] https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf.

[4] https://cppa.ca.gov/regulations/pdf/cppa_act.pdf.

[5] 7011(e)(1)(A) p.12. Agency- FINAL REGULATIONS TEXT (ca.gov)**.** It is important to note that a twelve month lookback period applies and therefore testing organizations should, for example, be prepared to honor requests from employees with respect to personal information collected from that date.

[6] The Superior Court for Sacramento County held that the plain meaning of the CPRA required that final regulations by the California Agency had to be in place by July 1, 2022 in order to allow them to begin enforcement on July 1, 2023. Accordingly, the court found that Agency regulations adopted on March 29, 2023 could not be enforced until March 29, 2024 and that any subsequently adopted regulations (including those related to the use of automated decision-making) could not become effective until one-year after their adoption. The court clarified that either the Cal AG or the Agency could continue to fully enforce the original CCPA Regs. The Agency has appealed this ruling.

[7] Two prior rounds of amendments to the CCPA Regs were released by the Cal AG in February and March 2020.

[8] https://www.gibsondunn.com/california-superior-court-halts-enforcement-of-certain-california-privacy-regulations/#:~:text=On%20June%2030%2C%202023%2C%20Sacramento,permitted%20enforcement%20of%20any%20provisions. This ruling was generally seen as beneficial to businesses, giving them additional months to comply with the updated CCPA Regs. **It is important to note that the enforcement delay to March 29, 2024 only applies to the updated CCPA Regs and not to the CPRA itself or regulations previously finalized under the CCPA.**

a. Applicability

For-profit enterprises doing business in California that meet certain criteria must comply with the CPRA. Prior Bulletins described the CCPA applicability criteria, which are modified by the CPRA as indicated below by italics:

- *As of January 1 of the calendar year*, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) *in the preceding calendar year*; or
- Alone or in combination, annually buys, sells, *or shares*, the personal information of *100,000* or more California consumers or households; or
- Derives *50% or more* of its annual revenues from selling *or sharing* consumers' personal information.[9]

Significant changes in the language determining which businesses are covered include:

1) Besides selling, sharing of personal information is now covered;
2) The volume of personal information processed annually is doubled;
3) The annual revenue reference period is specified as the prior calendar year;

As discussed below, "sharing" is limited to providing personal information to a third party for cross-contextual advertising. A business is not deemed to be sharing personal information where "*...A consumer uses or directs the business to intentionally disclose personal information or intentionally interact with one or more third parties."*[10] In any case, testing organizations should document in test taker agreements and privacy notices that personal information will be shared with institutions to which test takers direct scores are to be sent. Testing organizations with fewer than 100,000 candidates in California may find that the revised applicability requirements remove them from being a "covered business."[11]

b. Employment and Business Contact Data

The CCPA originally included temporary, two-year exemptions to most of its requirements for personal information collected from job applicants, employees, and contractors,[12] as well as for personal information obtained in conducting business with representatives of other organizations. Those exemptions were not extended under the CPRA and thus no longer apply as of January 1, 2023. Consequently, from that date employees and commercial business contacts are entitled to the same rights as other consumers.[13] As of that date covered businesses must meet all CPRA requirements for

[9] (SEC. 14. Section 1798.140(d)(1)) Californians for consumer privacy. Annotated text of the California Privacy Rights Act (As approved by voters). Annotated Text of the CPRA with CCPA Changes | CPRA Resource Center (caprivacy.org) Accessed 5/23/23

[10] SEC. 14. Section 1798.140(ah)(2)(B))

[11] And therefore outside of the scope of the CCPA/CPRA entirely. Sponsoring organizations offering specialized professional licensure exams may have a relatively select population of candidates to begin with, let alone in California.

[12] Among other personnel and as long as the personal information was used solely in that context.

[13] Among the states that have comprehensive consumer privacy laws currently in effect, only California extends privacy data protections to employees or business contacts.

such personal information.[14] That means the following steps, among other things, should be taken for employee and business contact personal information:[15]

- Updating privacy notices;
- Responding timely to consumer rights requests;
- Providing a clear choice to opt-out of sale or sharing of personal information; and

  Amending contracts with relevant service providers, contractors, and third parties.

c. Additional Consumer Rights and Details

The CPRA has expanded consumer rights and modified certain rights that existed under the CCPA.

Additional consumer rights added by the CPRA include:[16]

- the right to correct inaccurate information;
- the right to limit the use and disclosure of sensitive personal information; and
- the right to opt-out of automated decision-making technology.[17]

Under the CPRA, a consumer has a right to be informed at no cost about the personal information held by a business and its sharing practices.[18] The business must allow consumers to submit requests using a toll free number or via a website, hard copy by mail, or email. If a business only operates online, it can provide just an email address. The business cannot require the creation of an account to submit requests.[19] The business has 45 calendar days to respond to a consumer request.[20] If the consumer does not receive a response within this time frame, the individual can ultimately complain to the Agency. A business may deny the consumer's right to know for several reasons, including the inability to verify their identity[21] and if the business has provided the information twice already in the prior 12 months.[22]

---

[14] CPRA Effective 2023 Ending B2B and Employment Information Exceptions (natlawreview.com)

[15] Testing organizations also should note that the definition of personal information is expanded. In an employment context, it can include document metadata, photographs, network monitoring, and video surveillance. Biometric data – sometimes used for security access authentication, such as face or voice recognition, or fingerprint identification – could also fall into a PI category in some businesses.

[16] https://www.orrick.com/en/Solutions/CPRA ''

[17] The CPRA grants individuals the right to refuse profiling, i.e., the compilation of personal information to assess specific aspects of an individual's life or to analyze and predict elements such as work productivity, reliability and other behavior, and location. Of course, elements like productivity, interests, and reliability may be central to assessing individual suitability in employment contexts. However, the Agency has not yet adopted regulations governing such profiling.

[18] This includes understanding the specifics of information disclosure, categories of personally identifiable information (PII) collected, the collection purpose, categories of third parties involved, and the categories of information subject to business sales.

[19] If a consumer already has an account, the business can require that they log in before submitting a request.

[20] An additional 45 calendar days may be available if the business notifies the consumer an extension is needed.

[21] The business may require the consumer to provide verifiable proof of identity before disclosing the information.

[22] Frequently Asked Questions (FAQs) - California Privacy Protection Agency (CPPA)

A business is permitted to gather, utilize, and disclose personal information only to the extent reasonably essential and proportionate to the collection purpose. Collecting personal information for new purposes (different from the original notice) requires prior notification, including of the duration personal information may be retained.[23] The CPRA also provides clarity regarding requests for deletion of student-related data. **There is no requirement to comply with requests to delete a student's grades, scores, or test results. The Act also does not require a business to grant access to standardized educational assessments if this could potentially compromise the validity and reliability of those assessments.[24]**

d. Sensitive Personal Information

The CPRA introduced a new classification of "sensitive personal information", which includes social security, driver's license, state ID, and passport numbers, log-in credentials, financial account data, debit/credit card numbers, along with security codes or passwords granting account access.[25]

Covered businesses must notify consumers about the types of sensitive personal information collected, the purpose of collection, and whether the information is sold or shared.[26] **Consumers have a new right to instruct a business to restrict the use of sensitive personal information solely for necessary and expected purposes**.[27] Businesses must provide a "Limit the Use of My Sensitive Personal Information" link or have a unified "opt-out" link for the use, sharing or sale of sensitive personal information on their website, if processing sensitive personal information and subject to a number of exceptions in the CCPA Regs.[28] For instance, such an opt-out link is not required if a business is processing sensitive personal information to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services and to perform services on behalf of the business such as for providing customer service or verifying consumer information.[29] If a consumer decides to restrict the use or disclosure of sensitive personal information, the business must respect that choice for at least 12 months before again requesting authorization.

In practical terms, testing organizations should ensure operationalization of these new obligations through test taker agreements, privacy notices, website links and contracts with third parties.

---

[23] Three years is the maximum storage period following the conclusion of a contract or deactivation of an account.
[24] If these grades, scores, or assessments are considered part of the academic record under the Family Educational Rights and Privacy ACT (FERPA), they are already exempt from the CCPA and CPRA.
[25] See https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.140 for a full list. The CPRA specifies that the associated regulations will modify or supplement the categories of sensitive personal information, for example to account for technological advancements.
[26] Businesses cannot gather additional categories of sensitive personal information or use data for other purposes not initially disclosed without informing the consumer first.
[27] If the business uses or reveals this information for other reasons, it must inform the consumer and offer the choice to limit its use and disclosure.
[28] Alternatively, a consumer can adhere to the automated opt-out.
[29] See Section 7027(m) for all the exceptions to this notice and opt out requirement. Agency - FINAL REGULATIONS TEXT (ca.gov).

e. Party Roles and Contractual Language

The CPRA refers to the following parties that may have relationships with covered businesses:

1) Contractor (new) – a person to whom a covered business makes personal information available for a business purpose pursuant to a written contract;

2) Service Provider (modified) – a person that processes personal information on behalf of a covered business and that receives from or on behalf of the covered business personal information for a business purpose pursuant to a written contract;

3) Third Party (revised) – a person that is not the covered business itself, a contractor, or service provider. For example, a provider of cross-contextual behavioral advertising services or other business operations services (e.g., website data analytics).[30]

The updated CCPA Regs broadened obligations of entities engaged by a covered business and require specific language in contracts.[31]

Service Providers and Contractors are held to essentially the same requirements. They cannot retain, use, or disclose personal information collected in connection with a written contract with a business except in a finite list of specified circumstances, including for a specific business purpose set forth in the contract and by the updated CCPA Regs, or to retain another Service Provider or Contractor as a subcontractor.[32] The following table compares the contractual requirements for the three types of entities.

Contract Requirements	**Service Provider and Contractor**	**Third Parties**
Prohibit selling or sharing personal information	Yes	
Identify specific business purpose(s); specify that personal information is disclosed by business only for the specified and	Yes	Yes

[30] A cross-contextual behavioral advertising provider can only be a Third Party and not a Contractor or Service Provider. However, a Service Provider or Contractor may provide sales and marketing services directly related to the specific contracted purpose(s). For instance, a testing services provider might send targeted reminders to certificants or licensed practitioners of an approaching expiration date and the need to register for an exam, with options, pricing, etc. Such communications could perhaps include marketing information describing features and benefits offered by its services as well as demonstrated performance and comparative value as a preferred vendor choice. These purposes should be clearly specified in the agreement with a test sponsor organization beforehand.

[31] Analyzing the CPRA's new contractual requirements for transfers of personal information (iapp.org).

[32] Other permitted circumstances include for internal purposes to build or improve the quality of services provided to the business *even if not specified in the contract*, as long as the personal information is not used to perform services for another person, and to prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity, *even if not specified in the contract*.

limited purpose(s) set forth in contract		
Prohibit retaining, using, disclosing personal information for any purpose, commercial or otherwise, other than specified by contract	Yes	
Comply with all applicable sections of the laws and regulations; provide same privacy protection as required of businesses	Yes	Yes
Grant right for business to ensure personal information use consistent with covered business obligations, to stop and remediate unauthorized use, and be notified when contracted entity cannot meet obligations under CPRA	Yes	Yes
Enable business compliance with consumer requests	Yes	
Notify business of subcontractor & contractual compliance of subcontractor	Yes	

These contract requirements mean Service Providers and Contractors cannot sell or share personal information obtained from or on behalf of the business or received from other entities. The covered business is responsible for verifying that any personal information processed by Service Providers or Contractors is handled in compliance with the business's obligations in the CPRA and related regulations, and defined in their contractual agreements.[33] Testing services and contractor organizations should thus avoid using any data analytics applications or services to describe or understand client consumer groups (e.g., exam candidates) for any purpose before first obtaining legal advice. There should also be a written agreement indicating that the analytics vendor: (1) is a service provider under the CPRA; (2) will comply with all the CPRA requirements; and (3) will not sell or share any personal or sensitive personal information.

f. No More Opportunity to Cure

The CPRA removed the right for a business to cure a violation within 30 days of receiving a non-compliance notice. Consequently, any CCPA/CPRA violation is now subject to a risk of fine, with the opportunity to cure being subject to the discretion of the Cal AG.[34] Importantly, liability for violations now applies to Service Providers, Contractors, and any other person involved in collecting and processing personal information, not just the covered business.

g. "Sharing" v. "Selling"

[33] This may be accomplished by completing reviews, automated system scans, periodic internal or third-party audits, or other technical and operational evaluations carried out at least once every 12 months.

[34] The fine level is context dependent. The generally applicable fine is $2,500 per violation; however, this rises to $7,500 for intentional violations and those involving the personal information of minors (under the age of sixteen).

The CPRA introduced the concept of "sharing" personal information. Essentially, wherever the CCPA mentioned "selling", the CPRA adds "sharing."[35] As noted in the prior California Privacy bulletins, the disclosure of test taker personal information to testing service providers ought not to be considered a "sale" of personal information. This is now differentiated more clearly from "sale" by the modified definitions of Service Provider and Third Party.

The CPRA defines "sharing" personal information as "…communicating a consumer's personal information…to a *third party* for cross-context behavioral advertising, whether or not for monetary or other valuable consideration...". Important notes should be made here as follows:

1. "Sharing" is situationally limited to cross-contextual behavioral advertising;[36]

2. The definition of "sharing" refers to Third Party[37] rather than Service Provider. Therefore, vendors that are Service Providers are not within the scope of "sharing;"

3. Whereas "selling" personal information requires exchange of monetary or other valuable consideration, this is not a requirement for "sharing." We note that the definition of "sale" is very broad as it includes "other valuable consideration", which could be construed as a use of personal or sensitive personal information by a vendor for its own commercial purposes.

Testing organizations should review and update contracts with vendors to ensure they include the requisite language for such vendors to be considered service providers.[38]

h. Collection and Use Limitations

Bulletin 12 provided a summary of the CCPA notice at collection obligations. The CPRA makes changes to the requirements, including that a covered business must provide consumers with notice at or before point of collection of the following facts:

a. whether personal information will be shared or sold;
b. the data retention period (or criteria used to determine such period); and
c. additional disclosures regarding any collection and use of "sensitive personal information." [39]

[35] Equivalent updates are made in the CCPA Regs. For example, the CCPA prohibited a business from selling the personal information of a consumer under the age of 16 unless the consumer or the consumer's parent affirmatively authorized the sale. The CPRA adds "sharing" to this prohibition.
[36] "Cross-contextual behavioral advertising" is defined as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."
[37] A "third party" is neither the business, a service provider, nor a contractor. Therefore, a cookie provider engaged as a service provider or contractor and receiving personal information will not be considered as "sharing."
[38] Therefore any processing of personal information by such vendors should not be considered as being done pursuant to a "sale" or "sharing." This would be achieved by adding a prohibition on sharing personal information, in addition to existing prohibitions on selling personal information.
[39] The updated CCPA Regs also include new language addressing restrictions on the collection and use of personal information, including guidance on how organizations should determine whether collection purposes are consistent with reasonable consumer expectations. Testing organizations should review this guidance as they evaluate their collection of personal information practices.

Reflecting data minimization and purpose limitation principles similar to the EU General Data Protection Regulation, the CPRA requires covered businesses not to retain personal information for each disclosed purpose for any longer than is reasonably necessary to the purpose(s) for which it was collected.[40] The collected personal information can be used for another disclosed purpose that is compatible with the context in which it was collected, but not processed in a manner incompatible with those purposes.[41]

Testing organizations that are subject to the GDPR should be familiar with complying with the substance of these obligations. Others will need to spend more time evaluating their data collection practices to ensure these are not overly broad and beyond what is reasonable and proportionate for the express purpose identified.

i. Private Right of Action and Childrens' Personal Information

The CPRA makes a small number of changes to the CCPA private right of action. The unauthorized access and exfiltration of an email address (but not a username) in combination with a password or security question is added to the list of data elements that could give rise to a private right of action.[42] Putting in place reasonable security measures after a breach does not constitute a cure of that breach. As noted above, the level of penalties has also been modified by the CPRA with respect to personal information of children (under the age of 16) to $7,500 per violation, regardless of intent.[43]

ENFORCEMENT TO DATE AND FUTURE DEVELOPMENTS

The Agency now has administrative, investigative, and enforcement responsibilities, with the Cal AG having civil enforcement powers.[44] Published examples of enforcement activities to date, including in the areas of advertising technology, failure to honor opt-out rights and non-compliant notices, may help indicate regulatory priorities. As of the date of this Bulletin, the only enforcement activity resulting in a financial penalty is the $1.2M settlement between the Cal AG and Sephora. In that case, Sephora failed

[40] The CPRA also says that "[a] business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed..."

[41] The updated CCPA Regs provide guidance with respect to factors to consider when assessing whether another disclosed purpose of processing personal information is compatible with the collection context. The secondary purpose must be disclosed, i.e. it cannot be secret and then justified as compatible with the original collection context. The updated CCPA Regs confirm that a business shall not collect personal information categories other than those disclosed in its collection notice. If the business intends to collect additional personal information categories or use the personal information for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, the business shall provide a new collection notice.

[42] If breached and resulting from failure to implement and maintain reasonable security measures. Prior to the CPRA, the CCPA specified the following data elements as in scope: (1) social security number, (2) driver's license or other government identification number, (3) account number and any code or password that would grant access to a financial account, (4) medical information, (5) health insurance information, or (6) unique biometric data.

[43] If a minor or their parent or guardian does not consent to the sale or sharing of personal information, the business cannot ask again for twelve months or until the minor turns 16 years of age. Although these obligations apply based on the business actually knowing the child's age, willful disregard is deemed actual knowledge.

[44] It may be expected that going forwards the majority of enforcement activity will come from the Agency.

to recognize consumer opt-out rights and sold consumer personal information contrary to its own privacy policy.[45]

In addition to heeding lessons from published examples and the Sephora settlement, testing organizations should also be aware of the Agency's current rulemaking activities that will result in further regulations. As of the date of this Bulletin, the Agency is working on regulations that are expected to require certain businesses to perform annual cybersecurity audits and submit risk assessments, as well as addressing access and opt-out rights with respect to use of automated decision-making technology.[46] Testing organizations should review these regulations once they are finalized, and future regulations on other topics, to ensure their privacy programs address the relevant requirements.

CONCLUSION

The key updates noted at the beginning of this Bulletin provides a helpful summary of the main developments described here. Topics covered included revised applicability criteria, additional consumer rights, cessation of employment and business contact data exemptions, and the new concept of "sharing" personal information. Testing organizations and their vendors should carefully familiarize themselves with the changes introduced by the CPRA and updated CCPA Regs that are addressed in this bulletin, in addition to monitoring progress with further regulations to be published by the Agency shortly. Finally, it will be important to stay abreast of activities of the Agency and Cal AG with respect to enforcement, so that testing organizations can maintain a current understanding of regulator priorities.

[45] The Cal AG opened investigation against Sephora following a June 2021 enforcement sweep. In addition to CCPA violations, Sephora was found to have violated California's Unfair Competition Law, for making false or misleading statements related to the sale of personal information while unfairly depriving consumers of the ability to opt-out.
[46] The CPRA amendments to the CCPA directed the Agency to issue regulations on these topics. The Agency elected initially to focus on updating the original CCPA Regs to reflect the CPRA changes to the CCPA, before turning attention to authoring new regulations. Such future regulations will not become enforceable until twelve months after the date on which they are finalized.