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

Bulletin 12

January 28, 2021

COMPLYING WITH CALIFORNIA CONSUMER PRIVACY ACT

Review the regulations closely to ensure obligations are properly met.

This summary of key points is provided to facilitate review.

- The CCPA Regulations explain the main CCPA obligations but are complex and leave several key questions unresolved.
- Personal Information is defined broadly, but in ATP's view should not include derived test scores and results.
- Employee and business contact personal information is exempt from most requirements until January 1, 2023.
- Testing organizations should review and follow applicable CCPA Regulations details of consumer notice requirements.
- Testing services companies should ensure they meet the requirements to be considered a "service provider", including by entering into appropriate contracts with CCPA covered businesses.
- Consumer requests must be addressed in accordance with the CCPA Regulations, including response timeframes.
- Exchange of personal information between organizations in the administration, scoring and/or proctoring of a test should ordinarily not constitute a sale of Personal Information.

ATPSC International Privacy Subcommittee Members

Co-Chairs
Gary Behrens, FifthTheory
Donna McPartland, McPartland Privacy Advising

Members
Jamie Armstrong, Questionmark
Pamela Becker, Hogrefe
John Devoy, Proctorio
Andre' Kenji Horie, Duolingo
John Kleeman, Questionmark
Trushant Mehta, Open Eyes Technologies
Karin Merz, FGV
Allison Mulford, Prometric
Kathryn Myers, BTL
Robert Pryor, PSI International
Amin Saiar, PSI Services
Mike Sparling, MHS Assessments
Alex Tong, ATA
David Valentine-Elam, College Board
Marc Weinstein, Caveon
John Zarian, NCCCO

To read all published bulletins visit:
https://www.testpublishers.org/atp-security-committee-reports

For more information contact:
gary.behrens@fifththeory.com

OVERVIEW

This bulletin addresses the principal obligations for testing organizations to comply with the CCPA under the CCPA Regulations ("CCPA Regs"). The ATPSC International Privacy Subcommittee Bulletin 6 (December 2019) provided early guidance on the CCPA, which became effective on January 1, 2020. It addressed CCPA basic concepts and requirements, applicability, and other fundamentals. Review of that bulletin prior to reading to this bulletin will be helpful.

The CCPA Regs provide explanatory details regarding many of the main CCPA obligations. The final version of the CCPA Regs initially became effective on August 14, 2020; however, further modifications were proposed in October 2020 and then again on December 10, 2020. As such, the CCPA Regs are still apparently a moving target and ambiguity remains on a number of aspects. Accordingly, users need to monitor future developments that may result in additional changes. The text of the current CCPA Regs can be found on the California Attorney General website ("CA AG"). ATP's comments to the first version of the CCPA Regs are available in the Members Only area of the ATP website and remain valuable reference material (the "ATP Comments"). CCPA enforcement began as of July 1,

2020, with the CA AG declining to extend the date due to either COVID-19 or the absence of finalized CCPA Regs.

Users should also be aware of the California Privacy Rights Act ("CPRA"), which passed as a ballot initiative in November 2020 and will become the basis for a new law that will go into effective on January 1, 2023. Therefore, the information contained in this bulletin applies until that date (subject to any further modifications made to the CCPA Regs and to the CPRA's lookback provisions).

CONSIDERATIONS

Defining Consumer Personal Information

The definition of "consumer" under the CCPA and the CCPA Regs is broad, and not limited to an individual buying goods or services in-person. It encompasses any California resident[1] whose Personal Information ("PI") is processed by a covered business. Therefore, a test taker, a test administrator, a test proctor, and others who are California residents may qualify as consumers.

The CCPA Regs do not amend the definition of PI found in the CCPA. Bulletin 6 noted that inferences drawn from PI to create a consumer profile are included. Given this expansive view, there remains a question over whether test scores and results will be considered PI. The CCPA Regs provide no clarity on this point, which is unfortunate given that PI is a central legal concept, the definition of which needs to be reasonably clear for testing organizations to know how to comply.

ATP's position is that test scores and results, except for raw answers provided by test takers, should not be deemed as being PI. Test scores and results are the product of the testing process and are not information collected directly from test takers. Moreover, the policy reasons behind the CCPA are not reasonably applicable to the derivation of test scores and results; treating them as PI may cause significant problems for testing services.[2] Further discussion on this issue can be found in the ATP Comments (see above).

Employee and Business Contact Data

Two amendments signed into law in October 2019 exempted the collection of PI of business contacts, employees (including job candidates), and other personnel from full CCPA compliance until January 1, 2021.[3] As a consequence of the CPRA passage, the exemptions for employee and business contact purposes PI are extended until January 1, 2023.

[1] The CCPA and CCPA Regs also applies to PI of a "household", which is a key difference compared to other current prominent privacy laws, such as the EU General Data Protection Regulation. A household is defined as "a group" of consumers who cohabitate with one another at the same residential address and share use of common devices or services."

[2] To be clear, neither the CCPA nor the CCPA Regs provides any express assurance that test scores and results do not qualify as PI (at least unless they are de-identified by being anonymous or pseudonymous).

[3] In September 2020, these exemptions were extended until January 1, 2022, contingent on the outcome of the CPRA ballot initiative.

The CCPA Regs do not address how employee and business contact PI should be handled during the next two years. A logical assumption is that such information should be processed in accordance with the CCPA notice obligations (*see next section*) and existing legal requirements. Testing organizations – when acting as employers – should carefully review the definition of "employment-related information" in the CCPA Regs, and particularly the purposes of collection described in California Civil Code section 1798.145 (h)(1), to understand the scope of these exemptions and develop an appropriate notice to such individuals. Given that a period of time is needed to scope and implement new data handling practices, it is advisable to begin working towards compliance well ahead of January 1, 2023.

The CCPA Regs also do not address the situation of test sponsors and testing service providers processing the PI of employees, contractors, or job candidates of their business customers. Thus, it is not clear if and how the exemption applies to this type of PI. Because the exemption appears intended to apply to all otherwise covered businesses, it seems likely that employment-related information collected in this context may be exempt from most of the CCPA and CCPA Regs requirements. The CCPA Regs do indicate that links to a "do not sell" button and a privacy policy are not required in the notice provided to employees and job candidates at the point of collection.

The business contact PI exemption is most likely applicable in the context of communications with administrative contacts of customers (e.g., work telephone numbers, work addresses, and work email addresses). While the employee PI exemption applies for all of the substantive obligations of the CCPA and CCPA Regs, the exemption for business contact PI is not as broad.

Notice Obligations

The CCPA Regs provide further details on the content of notices to consumers required by the CCPA. Testing organizations should ensure their notices meet the relevant requirements. This bulletin does not, for reasons of brevity, address all notice issues.[4]

Notice at Collection: A core requirement for a covered business is to provide a "notice at collection of personal information." The notice must provide information on the categories of PI collected and purposes of use. Businesses should not collect categories of PI that are not disclosed in the notice, without first providing an updated notice. The notice must be easy to read (including on smaller screens) and to understand, avoid legal jargon, and be designed to draw the consumer's attention. The notice must be reasonably accessible to consumers with disabilities; when provided online it should follow generally recognized standards, such as the Web Content Accessibility Guidelines (WCAG) 2.1.

Importantly for testing organizations that are handling/processing consumer PI for their business customers, a business that does not collect PI directly from the consumer is not required in the CCPA Regs to provide a notice at collection so

[4] This bulletin also does not address privacy policy requirements. Many of the privacy policy requirements in the CCPA Regs mirror the requirements applicable to the notice at point of collection, including reasonable accessibility to persons with disabilities. Testing organizations should review § 999.308 of the CCPA Regs for further details on the specific contents that must be included in the privacy policy.

long as it does not sell the consumer's personal information.[5] Frequently a testing organization will directly collect the test taker's PI and only share it with its vendors/service providers (see Service Providers section below). However, in other cases this task may be delegated contractually to a testing service provider by the test sponsor. If a service provider collects the consumer PI, the service provider probably should provide the notice of collection. If a testing organization does not provide the notice at or before the point of collection, it must not collect PI. Consequently, the parties should discuss and agree how the PI is collected and who will fulfil the notice requirements.

Service Providers

A testing organization that provides assessment services (e.g., test development, test administration/scoring, proctoring services) to a covered business is most likely a "service provider." A business that collects PI directly from or about a consumer under direction of another business, and otherwise meets the requirements and obligations of a service provider, will be deemed a service provider.[6]

A testing organization that wishes to protect its role as a service provider should carefully review the requirements and obligations of the applicable CCPA provisions and CCPA Regs. For clarity, a testing organization that contracts for testing services should expressly agree in writing with its partners which of them is the covered business and which is a service provider. Although covered businesses have the principal compliance responsibilities, the CCPA Regs detail service provider obligations. Those include not using or disclosing PI except for the covered business and in compliance with the contract for services and other permitted purposes. Testing service providers should ensure they do not engage in activities that would result in being deemed a covered business and held responsible for complying with those obligations.

The CCPA Regs contemplate two possible responses to consumer requests to know or delete PI received by service providers: respond on behalf of the business or inform the consumer that it cannot act on the request. It would be advisable for testing services companies to specify in the written agreement with their customers an appropriate protocol and describe this in their privacy notices and terms. For example, the testing services provider should agree to promptly forward any such requests received to the covered business for response.[7] In other situations, a testing organization may be both a covered business and a service provider; an organization should inventory and map the PI it is processing to understand the role and responsibilities it has with respect to different data sets.

---

[5] Users should note that the California Online Privacy Protection Act ("CAL-OPPA") requires operators of websites and online services (including non-profits) that collect certain categories of PI about individual consumers residing in California to post a privacy policy. CAL-OPPA is applicable to organizations located outside of California.

[6] A testing services company may also be deemed a service provider if it provides services to an organization that is not a covered business, provided it meets the other requirements and obligations of a service provider under the CCPA and CCPA Regs.

[7] The testing services provider therefore needs to have proper processes for relevant employees to follow upon receipt of any consumer requests.

Consumer Requests

Testing organizations need to review the CCPA Regs requirements on consumer requests to ensure their internal policies and procedures comply, including with respect to the required contents of responses and verification of identity. Some key points are:

- *Request submission*: A testing organization operating exclusively online that has a direct relationship with a consumer from whom it collects PI must provide an email address for submitting requests to know about PI collected. All businesses have to provide two or more methods for consumers to submit requests to delete PI.[8]

- *Response times*: A request to know or delete PI must be acknowledged within 10 business days; the response to the request is due within 45 calendar days (plus an allowable extension). At least two communications with the consumer are therefore required.

- *Verification*: A testing organization must verify a requestor's identity before disclosing information and should inform the consumer if it cannot do so. The inability to verify the identity of a requestor is an acceptable reason to deny a request to know or to delete PI.

- *Denials*: Businesses may also deny consumer requests for other permitted reasons, including where providing PI would conflict with federal or state law, or would violate a legal obligation. For example, a testing organization may assert that information which would result in disclosure of Intellectual Property rights can be withheld (conflict with federal law), or when the testing organization is required by contract to retain PI for a legal challenge (conflict with a legal obligation), as well as when providing requested information may compromise the security of PI, business systems, and products.

- *Deletions*: Requests to delete PI can be handled by: 1) permanent and complete erasure of the PI on existing systems; 2) de-identification; or, 3) aggregation. Deletion of PI stored on archived or backup systems can be delayed until the system containing the PI to be deleted is restored to an active state or next accessed or used. The testing organization must tell the consumer whether it has complied with a request to delete; there is no requirement to confirm the method used.

Sale of Personal Information

Generally, testing organizations are not "selling" PI.[9] Instead, testing organizations may contract with service providers to administer, score, and /or proctor tests where test taker PI needs to be processed for those purposes (see Service Providers section above). Whether sharing PI with affiliates and other

[8] Businesses must consider the methods by which they primarily interact with consumers when deciding how to deal with requests.

[9] "Sale" is defined broadly to include disclosing, transferring, and making available consumer PI to another business or third party for monetary or other valuable consideration. The CCPA Regs do not define "other valuable consideration" or discuss how consideration in service provider contractual agreements differ from an exchange for sale.

business partners that provide services constitutes a sale is somewhat murky (but see discussion in the next paragraph and in the Service Providers section above). Arguably such sharing should not be a sale, at least for necessary providing of test results and scores under contracts. This may be particularly true where an employer pays for a test and is provided with the test results by the testing organization, with the employee's/applicant's knowledge. Thus, it is advisable to obtain an acknowledgement from the employee, job candidate, or other test taker that results will be shared with the employer (or similarly for sharing results with certification bodies).

Each testing organization should evaluate the definition and use of "sale" compared to its particular circumstances. The CCPA Regs specify certain situations that are not sales, including where a business uses or shares with a service provider PI of a consumer that is necessary to perform a business purpose. This is conditional on the business having provided notice of that information being used or shared in its terms and conditions.[10] For many testing organizations, this exclusion would apply to test taker PI that is disclosed to one or more testing services provider(s) that are involved in the overall testing services as contractors/vendors.[11]

All testing organizations also should more broadly review their PI sharing practices, including their websites, any targeted advertising and other marketing activities, to determine whether any of these activities qualify as a sale.[12] If there is a sale, the business must provide a notice of such selling and the right to opt-out. A business selling PI must also provide a "Do Not Sell My Personal Information" link on its website homepage to an internet page that enables the consumer to opt-out.[13] Testing organizations that determine they are selling PI should carefully review the required elements of the opt-out notice, including the December 2020 CCPA Regs revisions which suggest a form of additional opt-out button. If a testing organization is not selling PI, it does not need to provide an opt-out and should state in its privacy policy that it does not sell PI.

Enforcement/Private Right of Action

The CCPA Regs add no further details on these matters. What is important to know is that enforcement by the CA AG is now occurring, and as set forth in

[10] It also demands that the service provider does not further collect, sell, or use the PI except as necessary to perform the business purpose and other reasons as specified by the CCPA Regs.

[11] This will be a context specific analysis for testing organizations. For example, provision of test information for educational research and test validation or psychometric purposes should be addressed in the test sponsor's contracts and privacy notices to test takers. There are other particular purposes where it is important for the parties involved in the test administration to clearly document their respective roles and responsibilities, such as responsibility for obtaining test taker consent and "do not sell" notice obligations where it is determined that PI sharing is likely a sale (e.g., test taker opt in authorizing sharing of test results for purposes of colleges and university recruitment).

[12] Note: this bulletin does not address specific issues associated with test takers under age 16, in respect of which opt-in consent is required for the sale of PI.

[13] Any sale of PI must also be described in the organization's privacy policy.

Bulletin 6, there are potential fines for violations. A limited private right of action is available to consumers for violations of the breach notification provisions. Once the CPRA becomes effective on January 1, 2023, a new state agency will be created to enforce the law. Class actions are frequently filed in California under its Unfair Competition Law and these actions are more frequently including claims under CCPA, including the security and data breach notification private right of action.[14]

Training/Record Keeping

A business must inform its personnel responsible for handling consumer queries about its business practices and CCPA compliance in respect of all of the requirements in the CCPA and CCPA Regs. Records of consumer requests and how these were responded to must be retained for 24 months. Otherwise, businesses are under no general obligation to retain PI solely to comply with consumer requests. There are obligations to keep and disclose annual metrics that will likely only impact businesses that are larger in size or that process higher volumes of PI.[15]

CONCLUSION

This bulletin, along with Bulletin 6 and the ATP Comments, provide specific information related to testing organizations' obligations with respect to the CCPA. In summary, while the CCPA Regs provide some helpful clarity and details as to how to interpret and implement the law, other questions (e.g., whether test scores are considered PI, revenue-based applicability of CCPA criteria) remain uncertain. The language of the CCPA Regs themselves is fairly abstruse and difficult to read, so clear guidance is not available in every instance. Still, the CCPA Regs remain the best source of assistance for testing organizations seeking to better understand how to comply with the CCPA – at least until some initial enforcement actions are taken and cases are decided that may provide more clarity.

[14] See the IAPP CCPA litigation tracker.

[15] A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the PI of 10,000,000 or more consumers in a calendar year is required to compile detailed records regarding CCPA requests it receives.

