BEFORE THE CALIFORNIA DEPARTMENT OF JUSTICE

California Code of Regulations, Chapter 20, Title II, Div. 1 (sections §§ 999.300 - 999.341)

Comments of the Association of Test Publishers

The Association of Test Publishers ("ATP") submits these comments to address the serious concerns of the testing industry about the Proposed Regulations for implementing the California Consumer Privacy Act ("Proposed Regulations"), as published on October 11, 2019. This submission is being made by the required date of December 6, 2019.

The ATP is the international trade association for the testing industry. The ATP is comprised of hundreds of publishers, test sponsors (i.e., owners of test content, such as certification bodies), and vendors that deliver tests used in various settings, including healthcare, employment (e.g., employee selection and other HR functions), education (e.g., academic admissions), clinical diagnostic assessment, and certification/ licensure (e.g., licensure/ recertification of various professionals), and credentialing, as well as businesses that provide testing services (e.g., test security, scoring) or administering test programs ("Members"). Since its inception in 1987, the Association has advocated for the use of fair, reliable, and valid assessments, including ensuring the security of test content and test results. Our activities have included providing expertise to and lobbying the US Congress and state legislatures on proposals affecting the use of testing in employment and education, as well as representing the industry on regulatory matters and litigation surrounding the use of testing. We developed and currently publish compliance guidelines on the EU General Data Protection Regulation ("GDPR") and are currently publishing a series of educational bulletins entitled, "Privacy in Practice" that focus on compliance with both US and international privacy laws and regulations.[1]

The ATP respects the goals of the Proposed Regulations to ensure comprehensive implementation of the California Consumer Privacy Act ("CCPA") and to provide guidance to businesses that must comply. However, we strongly believe that specific circumstances common in the testing industry, along with the many smaller/medium-sized businesses in the industry, justify modification of the Proposed Regulations when balanced against the rights of individual test takers as consumers. Thus, the ATP urges the Attorney General to take these specific comments into account in adopting final regulations.

---

[1] The ATP is preparing to publish a bulletin on compliance with the CCPA yet this month. Another pending bulletin focuses on the use of international standards by testing organizations to achieve data security and privacy objectives (i.e., ISO 27001, ISO 27701), as well as the use of third-party audits that are performed under AICPA (American Institute of CPAs) standards for Systems and Operational Controls (SOC) Reports. *See* discussion of "reasonable security measures," *infra.* at p. 18.

Many testing events occur which greatly benefit and protect the general public, along with those who rely on test results, especially individual test takers. California consumers are no exception to the vast – and growing – population of users of assessments whose purpose is to advance themselves personally and/or professionally.[2]

Individuals voluntarily submit to being tested for many reasons. Among them is to obtain a driver's license, to identify ways to improve their lives, to understand their academic strengths and weaknesses, to gain admittance to an institution of higher learning or other academic/adult educational program, to seek employment or to gain a promotion once employed, to become licensed/certified in a profession, to become certified in sport/recreation (e.g., flying, scuba) or professionally (e.g., IT certifications in literally thousands of technical skills), and even to understand their own health (e.g., diagnostic tests) or how to provide lifesaving procedures on others (e.g., CPR). In a majority of these instances, assessments are pivotal to a public interest and/or consumer protection motive (e.g., medical, legal, accounting, airline pilot, police, EMT).

Many of these situations are examples of "high stakes" secure testing, i.e., where the outcome of a test carries a significant consequence for the test taker (such as a securing a job, getting admitted to a school, or being issued a license or certificate). In these cases, the test items are kept secure (even by the U.S. Copyright Office, which has separate copyright registration procedures for secure tests) to ensure that future test takers cannot obtain advance knowledge of them – which would have the effect of invalidating the test results. In fact, if some test takers are able to obtain favorable results on a test by cheating then the value of the testing program is completely undermined for everyone. Testing has become part of our daily lives; individuals generally well understand that testing provides them with benefits, directly or indirectly, by assisting to serve the public health, safety, and welfare of the community or society as a whole.

Thus, it is vitally important that every high stakes testing program is able to ensure that its online registration process can be conducted in accordance with the CCPA and that all test administrations, whether conducted in person or online, are fair to all test takers. In so doing, a testing organization must be able to ensure that an individual who takes a test is in fact the same individual who is registered to take the test (with or without establishing that s/he is eligible to take the test). Furthermore, testing organizations must monitor testing events to ensure that

---

[2] The ATP's comments are not intended to apply to educational testing in K-12 classrooms However, the ATP is aware that some school admissions testing of children is done by computer, as well as career-oriented K-12 educational and vocational education programs for children. In any situation involving the testing of minors, including for medical/diagnostic purposes, the ATP expects that the controlling business would require a test taker agreement to be signed by the parent, inasmuch as minors do not have legal status to enter into such an agreement. Thus, regardless of age of the minor child, the ATP requests that the final regulations (§999.330-332) be modified to be consistent with this legal requirement. We submit that if there is an effective "affirmative authorization" by a parent or guardian in the first instance, there is no need for any separate opt-out notice to the child or a separate opt-in process.

administration irregularities which may have an adverse impact on every test taker are detected and handled in an appropriate manner.[3] Equally important, testing organizations seek to ensure that all personal information collected from test takers (i.e., "consumers") is protected from unauthorized access and/or acquisition, and that all privacy-related requests from consumers are handled appropriately under the terms of the relevant laws. For all of these reasons, the ATP submits that every high-stakes testing organization has the following legitimate purposes associated with the need for collecting and using the personal information of test takers: (1) to ensure fairness in testing; (2) to prevent fraud (i.e., cheating) by individuals taking a secure test; and (3) to protect proprietary (and often copyrighted) secure "high stakes" test items from being stolen by test takers and illegally distributed to future test takers.

Consistent with the above objectives, the ATP notes that many high stakes testing programs are national in scope, drawing test takers from every state.[4] For ease of business operations, ATP Members often adopt a uniform Privacy Policy to meet the needs of all test takers across the United States. Given the upcoming effective date of the CCPA, we understand that many testing organizations have already modified their privacy policies to meet the CCPA requirements. Thus, it is very important to ATP Members to be able to manage their operations to address all aspects of the CCPA while complying with other applicable state privacy laws. Through its comments, the ATP has addressed testing-specific issues to highlight interpretations and recommended ways to modify the Proposed Regulations.

General Background – Roles and Responsibilities in Testing

At the outset, we need to make the Attorney General aware that a majority of the high stakes testing programs do NOT rely on a traditional two-party business relationship, where a

---

[3] It is important to recognize that in most high stakes tests, the test-taker is expected to answer questions on his/her own, without having advance access to test questions, receiving any assistance from another person, by using reference materials or notes, or having unauthorized access to the Internet. Obviously, these high stakes tests are unique to the specific individual taking the test – the results/scores are only intended for and relevant to the specific individual who has registered for the test and then verified to take the test. Consequently, every testing organization pays significant attention to the security of test content and test taker information, to ensure that cheating on tests is prevented so that every test taker has an equally fair opportunity to succeed.

[4] Indeed, many ATP Members operate international testing programs, meaning that those organizations register and administer tests to foreign test takers. Thus, they must operate in accordance with foreign privacy laws, especially the General Data Protection Regulation ("GDPR"). In those situations, many ATP Members have attempted to establish a uniform privacy policy that harmonizes the GDPR with the CCPA. It is unrealistic to expect an entity doing business internationally to adopt completely separate and distinct privacy policies for each country in which it operates (or for each state in the United States).

consumer has a direct relationship to the business that is selling goods or services (e.g., going into a store or online to make a purchase directly from a seller). To accomplish smoothly functioning and efficient operations to serve their customers, many testing organizations have segmented their operations into two or more diverse roles in the provision of testing services: one entity that owns the test (that may have developed the test or contracted for its development) and makes all of the decisions about how to use any personal information obtained from an individual test taker; and one or more secondary entities that actually handle the delivery, administration and scoring of the testing services. It is such a secondary entity that in many instances is the one that actually has the direct contact with the test taker/consumer.[5] In addition, there often are other parties who provide supporting services to either or both of the two principal businesses (i.e., function as a "service provider" under the CCPA). The final regulations must recognize that any business that functions as a "service provider" does not control the collection and use of consumers' personal information.[6]

Another unique factor of the high stakes testing industry is that "consumers" of tests and testing services may be individuals, but in many instances, the rights to use tests and/or testing services are "sold" to businesses (i.e., employers) or professionals (e.g., doctors, psychologists), who then have the responsibility to arrange for the administration of the tests to the actual test takers, either by themselves or by a test delivery vendor. In this context, then, it is equally important to note that, especially for "secure tests" (i.e., those tests whose items must not be made available to test takers in advance of a test administration), the tests themselves are not "sold" in the commercial sense, but are provided for use by the customer of the testing services – ownership of the tests is not conveyed in a commercial "sale."[7]

---

[5] Under the GDPR, these parties are labeled as the "controller' and the "processor." The ATP encourages the Attorney General to adopt these terms or at least provide equivalent definitions by making use of similar parallel terms, both for the sake of clarity and to enable consistent treatment of personal information by entities that must comply with both the CCPA and the GDPR. Without clarification in the final regulations, the ATP fears that the CCPA could be interpreted as placing a higher regulatory burden on the processor/service provider than it does on the controller.

[6] Thus, the ATP generally endorses the Proposed Regulations regarding "service providers" (see §999.313), although we have recommended clarification of these regulations, as addressed in Section 7 (*see* in*fra.* at pp. 21-23).

[7] Secure tests are granted special copyright protection in the United States under the 1976 Copyright Act. The regulations implementing the Act define (in part) a ''secure test'' as ''a nonmarketed test…" "For these purposes, a test is not marketed if copies are not sold but it is distributed and used in such a manner that ownership and control of copies remain with the test sponsor or publisher.'' 37 CFR 202.20(b)(4). [FOOTNOTE CONTINUED ON NEXT PAGE]

Perhaps because of the complexities inherent in the provision of testing services, the standard practice for most testing organizations is the use of a formal test taker form/agreement to spell out to each individual test taker both his/her rights and responsibilities related to the testing services (e.g., rights to challenge or appeal, retest rules, prohibitions on copying/sharing test items), as well as the information about the business's privacy policy, which the consumer must acknowledge or accept.[8] Among the uses of personal information that may be enumerated in such agreements are specific steps taken to ensure that cheating does not occur (e.g., monitoring test administration either physically or electronically). Many testing organizations require the test taker to sign this agreement first when registering online for the test and then again at the test administration before the test taker begins the testing session, which provides evidence that the test taker was given the required notice twice.

Because of the well-documented division of responsibilities among different entities participating in a testing event, the most critical issue in a privacy context is which entity has the responsibility for collecting personal information from test takers and for determining what use(s) are to be made of that information, which usually is the test owner. While the high stakes test owner may obtain test taker information from one or more of its service providers in the performance of the testing services, the responsibility for compliance with the CCPA must fall squarely on the test owner, the entity that makes all of the relevant decisions about what personal information should be collected and what uses it makes of that personal information.[9]

Equally pertinent to this issue is the key distinction between test takers' personal information (e.g., name, address, email address) and the outcome of testing services purchased by the test takers – the test results or scores. Although it may be appropriate in some situations to recognize that the answers to test items given by a test taker are "personal" to that individual,

---

See 42 *Fed. Reg.* 59,302, 59,304 & n.1 (Nov. 16, 1977). The ATP contends that the final regulations must include guidance on an exception addressing the recognition of a business's IP rights under federal law.

[8] The ATP believes that, to the extent that a test taker form/agreement is used by a testing organization as a "point-of-collection notice," it must meet the requirements of §999.305(a). Nevertheless, no matter how much a business tries to use "plain language" and "avoid legal jargon," someone can always assert that a document fails to conform. The final regulations should be modified to include language that a notice shall be "reasonably written to achieve the goals" to ensure that a balanced approach is used to evaluate all such documents.

[9] Of course, some of those responsibilities may be delegated by contract to one or more service providers, who often times have the direct relationship with the test takers, such as handling registration of test takers, administering the actual testing services, scoring tests, and/or managing the security of the testing event. *See* discussion of "data broker" *infra.* at p. 23.

test results/scores are not "collected" information. [10] Test results/scores are the product of the test services procured by the consumer; they are not information collected from test takers, but are derived outcomes produced by the testing organization using proprietary scoring rubrics.[11]

Moreover, the uses of test results/scores are co-extensive with the need of each test taker for the testing services. In other words, if an individual is seeking a license/certificate documenting a particular skill (e.g., in law, medicine, technology), the issuer of that license/certificate is the owner of the test and the outcome is based on the individual's test results/score; similarly, if an individual is seeking a job or a promotion, that decision is made by the employer, based upon various factors, including the individual's test results/scores. Application of overly-prescriptive privacy requirements on the sharing of an individual's test results/scores defeats the very purpose the individual had in taking the test in the first place.[12]

Another issue related to test results/scores is raised by the CCPA definition of "personal information" to include "inferences" drawn from any of the information identified to create a profile about a consumer; specifically, the law addresses inferences about a consumer's: preferences; characteristics; psychological trends; predispositions; behavior; attitudes; intelligence; abilities; or aptitudes. *See* Cal. Civ. Code §1798.140(o)(1)(K). The ATP submits

---

[10] Even "raw" data provided by a test taker is not always considered to be "personal information" or treated as personal information. In circumstances where the test taker is an employee, where the testing organization's IP rights must take priority over a person's test answers, and where other exemptions may exist that supports a denial of a request for access to, or deletion of, information collected from the test taker, such test answers are effectively not personal information . These situations are covered in the test taker agreement (*see infra.* fn 10).

[11] Significantly, this type of derived information is largely unique in the testing industry. Test results/scores are distinguished from consumers' input on social media services, where an individual's postings to the platform are then shared in the same manner and context in which they were inputted. Nor are testing results/scores remotely similar to derived personal information that is generated in a marketing context, where a person's buying patterns/behaviors are tracked and used to create a profile that is sold to other marketers. Indeed, the Proposed Regulations (at §999.305(d)), make it clear that such results cannot be "personal information at the time of collection" – obviously, test results/scores do not even exist at the time of collection of the consumer's personal information related to the testing services. An individual acquires (or obtains) testing service where test scores are the contracted for outcome or product. What a testing organization does with those scores is governed by and disclosed to the test takers in the test taker agreement.

[12] This is true regardless of whether the individual paid for the test; in some instances (e.g., employment, training) the employer may have paid for the test. Even when an individual pays for the test, s/he authorizes the test owner to share the results/scores with certain designated recipients (e.g., schools to which the individual is applying, jobs for which the individual is applying, certification bodies from which the individual is seeking a license or certificate). Either way, the need for a decision-maker, or multiple decision-makers, to obtain the test results/scores is precisely the reason why the individual registered for and took that test.

that if the CCPA is implemented with extreme interpretations, it would effectively ban all of the testing services we have discussed. Rather, we believe that the CCPA is focused on regulating the sale of consumer marketing profiles to other marketers, not preventing consumers from obtaining testing services they themselves consider valuable. Read in this light, then, the final regulations should articulate this distinction and establish the clear focus on the uses of personal information for consumer marketing activities, not the prevention of legitimate business service outcomes.

Another reason for our concern about the treatment of test results/scores stems from the definition of the term "sale" under the CCPA. The CCPA defines the "selling" of personal information broadly to mean a business selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information to another business or a third party for monetary or other valuable consideration. Unfortunately, neither the CCPA nor the Proposed Regulations defines what qualifies as "other valuable consideration." It is absolutely crucial that the Attorney General establish a proper definition in the final regulations, clarifying what is "valuable consideration" in specific contexts. Without such clarity, a testing organization that shares a "common interest" in scoring and reporting test scores of test takers with its affiliates, subsidiaries, service providers, contractors, or other business partners ("vendors") (i.e., the controlling business must share personal information in order to fulfill its contractual obligations to provide testing services – especially the test results/scores on a test), inappropriately may be deemed to be violating the CCPA. The ATP contends that such "common interest" sharing does not constitute "valuable consideration" inasmuch as test takers' results/scores are only shared to further the underlying testing service contract and they do NOT result in any commercial value related to any marketing of personal information to these other businesses.[13]

In advancing these positions regarding privacy notices, the ATP affirmatively agrees that a testing organization that uses test takers' personal information, including any test results/scores, for advertising/marketing purposes, or shares such information with a vendor in a way that permits the vendor to commercially use that information, must comply with the CCPA requirements as related to such purposes.[14] Therefore, when a testing organization wants to communicate with previous test takers to promote or market its products or services (e.g., new

---

[13] In most situations, the testing organization's contract with a vendor specifically restricts the use of any personal information shared pursuant to the contract to the services required. In other words, the vendor is not allowed to use that personal information for its own business purposes outside of the services being provided under the contract with the controlling business. It is that third-party commercial marketing that the CCPA intends to regulate, not the ability of vendors to provide legitimate services in the fulfillment of an underlying contract.

[14] By comparison, it should be abundantly clear that communicating with a consumer about his/her current contract for testing services (e.g., providing details about which test and the test location or date), is expected as part of a current contractual relationship and does not constitute marketing.

testing products or companion testing opportunities not already involved in a services contract), those communications constitute marketing and the business must comply with the CCPA.

This background information on the roles and responsibilities as found in the testing industry relate to specific Proposed Regulations, as addressed in the following comments.

Comments on the Proposed Regulations

1. Issues in determining if a testing organization is covered.

Two fundamental issues confront a testing organization in determining if it is covered under the CCPA: (1) whether it has more than $25 million in gross revenues; and (2) whether it collects personal information on more than 50,000 California consumers. Moreover, parent companies and subsidiaries using the same branding are covered in the definition of "business," even if they themselves do not exceed the applicable thresholds – the ATP objects to this determination on the grounds that if the parent/subsidiary is itself a separate legal entity, it is lawfully entitled to be treated as a separate business. The final regulations should rectify this mistaken legal position.

Despite extensive debate since passage of the CCPA as to whether the appropriate revenue threshold is "California revenues" or total revenues of the organization for all of its operations, the Proposed Regulations are silent in resolving that question. Because a testing organization may have total gross revenues that exceed the $25 million threshold on a national or even international basis, but generate less than that amount from selling testing services to California consumers, resolving that question is extremely important for the testing industry. In other words, a business may engage in test development and other consulting services completely outside of California that do not involve the collection of personal information of California consumers or any commercial marketing of their personal information collected by others. We submit it would be unfair to hold a business liable to comply based on revenues that are not related to the legitimate consumer privacy purposes of the CCPA. In those situations, the ATP submits that the business is not subject to the CCPA.[15] We request that the final regulations address both of these possibilities to clarify the appropriate scope of the CCPA.

Turning to issues over the threshold involving the number of consumers, many testing organizations, whether they are controllers or processors (service providers) of test takers' personal information, may have no way to determine if they have records on more than 50,000

---

[15] Thus, any interpretation of this threshold test that interferes with and/or creates a burden on interstate commerce is invalid under the Commerce Clause of the United States Constitution. (Article I, Section 8, Clause 3), which gives to Congress the exclusive power to regulate commerce "between the several States." This is true regardless of whether the entity is located in California or outside of the state.

California consumers. The ATP has already heard from some of its members that, especially when functioning as a service provider (e.g., providing test delivery and/or scoring services), test takers' physical addresses are not always used, which therefore makes it impossible to determine the consumers' state of residence, and consequently, whether the testing organization meets the threshold.[16] This lack of physical address is also likely if the testing organization uses only a coded (or tokenized) identifier. Accordingly, the ATP requests that the final regulations acknowledge that the inability to determine (either physically or electronically) the number of California consumers in a database will not in itself be interpreted as a violation of the CCPA – or will not result in an automatic assumption that the business is covered.

2. **Issues concerning "point-of-collection" notices.**

As noted above, a testing organization that acts as a controller may not actually collect test takers' personal information, rather it is most often collected by one or more service providers (e.g., website operator, payment gateway, testing services vendor). That practical reality leads to concerns about how Privacy Notices are to be handled under the Proposed Regulations.

While §999.305(a)(1) sets forth the "general principle" that such notice "is to inform consumers at or before the time of collection of a consumer's personal information of the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used[,]" nowhere in this regulation, nor in the CCPA itself, is there a requirement as to who has to provide the notice. As such, the ATP submits that a valid "point-of-collection" notice should be able to be provided to a specific consumer by either the controlling business or by its service provider(s) under contract. We urge the Attorney General not to lose sight of the crucial general principle – as long as the appropriate notice is given to consumers (here test takers) prior to the collection of personal information, it should not matter whether that specific notice is given by the owner/sponsor of the test/test program, who makes the decisions about the purposes and uses of the collected information, or by a service provider working under contract to the test owner that may actually have the direct contact with the consumers.[17]

---

[16] Many organizations operate national or international online testing programs, where typically test takers are only identified by full name and email address, but since there is no need the physical address, it is not captured. This is particularly the case when an entity follows privacy minimization guidelines. Moreover, a single testing organization may have multiple customer contracts and thus not know—or have any ability to ascertain—how many California consumer records it has (e.g., 50,000 or 4 million).

[17] The Proposed Regulations state that, "If a business does not give the notice at collection to the consumer at or before the collection of their personal information, the business shall not collect personal information from the consumer." §999.305(d). The ATP recommends that this sentence should be modified to acknowledge [FOOTNOTE CONTINUED ON NEXT PAGE]

Similarly, the Proposed Regulations (§999.306(d)) also state that a business is not required to provide a "point-of-collection" notice when it collects personal information from a third party and not the individuals themselves. But in such situations, the Proposed Regulations require that the controlling business cannot "sell" such personal information unless it goes through another step to ensure that the appropriate notice was in fact provided by the third party. As we noted earlier, the controlling testing organization is NOT selling or making any commercial use of personal information, but is using/sharing it with its vendors to fulfill an ongoing test services contract with the consumer directly or through another entity that has a contractual relationship with the consumer (e.g., an employer, a certification body from whom the consumer is seeking to earn a certificate, credential, or license) – and equally important, to notify the consumer about the test results.[18] Forcing the controlling test owner/sponsoring program to perform one or more extra compliance steps beyond the underlying contractual obligations of the parties is onerous, time consuming, and therefore represents an unnecessary cost to all of the businesses involved – plus, it provides no additional benefits or rights to the consumers/test takers. The approach seemingly mandated by the Proposed Regulations elevates form over substance – the rights of the consumer under both the CCPA and §999.305(a)(1) are met when any one of the businesses with a legal obligation, as agreed to between them, gives the notice.

An important inconsistency in the Proposed Regulations arises when the initial point of contact is online. This problem is significant for testing organizations, where the great percentage of consumer registrations for testing services occurs online. The Proposed Regulations (§999.306(d)) state that a "consumer whose personal information is collected while a notice of right to opt-out notice (sic) is not posted shall be deemed to have validly submitted a request to opt-out." First, such an assumption is unwarranted – just because a business collects personal information does not mean it is selling that information. Moreover, that assumption expressly conflicts with the statement immediately following, that a business does not have to post an opt-out notice if it is not selling personal information. In contrast, though, §999.315(c)

---

that any business involved in the "common interest" use of the consumer's personal information should be permitted to give notice. If the consumer does not opt out in response to such a notice, s/he has opted-in to the collection and use of personal information – this is an "affirmative authorization" as defined in §999.301(a).

[18] Sharing or "selling" personal information in an employment testing situation is often a total misnomer. When the employer is paying for the test, with the employee's obvious knowledge, the testing organization is under contract with the employer and the test taker's personal information is shared directly from the employer with the testing organization. If the test results for specific employees were not allowed to be shared as part of the contract, no testing services could be provided. The ATP submits that the Proposed Regulations should not be interpreted in such a manner as to prevent specific business contracts from being entered into and performed – and the final regulations need to make this point clearly.

of the Proposed Regulations requires that if a business collects consumers' personal information online, it "shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid ["do not sell"] request … for that browser or device, or, if known, for the consumer."[19]

As related to the testing industry, neither requirement makes sense. A test taker who registers for a test online is not likely to opt-out of the collection of his/her personal information, without which the testing services cannot be delivered, including the delivery of the test results/scores. If a test taker were to opt-out of the service, the testing organization would be unable to share the test taker's information with its "common interest vendors" and the testing services would not be able to be fulfilled. Similarly, a test taker who needs his/her test results shared to apply for a job/promotion (i.e., shared with an employer) or to obtain a desired certificate, credential or license (i.e., shared with a certification board or state licensing board) is not likely to tell the controlling testing organization not to share the test results – that is the whole point of taking the test.[20] On this point, users of test results/scores are not going to take the word of the test taker as to his/her scores; that information must come from the issuer of the results/scores to be assumed valid.

Additionally, in the conduct of its testing services, it is vitally important that the testing program is able to collect specific video or biometric information (e.g., photo IDs, fingerprints), to ensure that an individual who appears for a test session is in fact the same individual who is registered to take the test (with or without establishing that s/he is eligible to take the test), and furthermore, that its testing events are adequately monitored and controlled at the testing location (e.g., secure test center) or at home, and that testing irregularities which may have an adverse impact on every test taker are detected and handled in an appropriate manner .

---

[19] Even if a testing organization wanted to comply with either of these requirements, it is practically impossible given conflicts in the Proposed Regulations. In §999.305(b)(3)) the business is required to the provide the consumer with a link to access "an interactive webform" where consumers can exercise their rights, while §999.305(c) requires the link to redirect individuals to the relevant portion of the business's privacy policy. This inconsistency needs to be rectified in the final regulations.

[20] The timing of a consumer's decision to opt-out also plays a significant role in a testing organization's handling of the matter. On a procedural level, it is impractical to opt-out after the test taker has already taken the test because it would result in inappropriate and dangerous outcomes for a testing organization to permit a consumer to opt out after a test has been taken or scored. Either outcome would be tantamount to allowing the test taker to delete his/her test results because the score was too low or cheating by retaking the test after seeing the items and then "deleting" the first score – a test taker using either "opt-out" could not receive a valid score or would be engaged in an attempt to cheat on a future test.

Finally, the Proposed Regulations fail to take account of the recent amendments to the CCPA in regards to the respective one-year exemptions in the treatment of employees' personal information and business contacts' personal information. As explained below, it is important to members of the testing industry that appropriate guidance regarding those changes be included in the final regulations.

a) Need for guidance on handling employee personal information.

The Legislature passed an amendment providing a one-year moratorium on the treatment of employee personal information, which is not reflected in the Proposed Regulations. The ATP strongly encourages the Attorney General to address this situation in the final regulations by setting forth specific guidance as to how a business should handle relevant employee personal information during the moratorium, especially with regard to the notice of collection that it provides to its employees and other affected individuals.[21] Of course, testing organizations are themselves employers that must keep and utilize employee information in the course of meeting state laws, insurance requirements, and the like. As such information retained by the business is NOT consumer related, and should not be regulated by CCPA.

More than testing organizations as employers, we note that to the extent testing organizations provide testing services, a business employer customer is often the controlling entity in determining what personal information is collected from its employees and how it is used in regards to a particular test used for internal HR decisions. Since this delay applies to all businesses that may otherwise be covered, it is critical that this guidance be made available as quickly as possible.

In the context of privacy notices for employees, job candidates and contractors some requirements in the Proposed Regulations ("do not sell" and website privacy links) appear to be inapplicable at this time; the final regulations should reflect the exemptions, or explain how the moratorium should be implemented for 2020.

b) Need for guidance on handling business contact information.

The September amendments also contained a one-year moratorium on the treatment of business contact information. That amendment is of importance to the testing industry because in many situations, a testing organization is selling tests/testing services not to individual test takers, but to employers and/or others (e.g., doctors, counselors) who in turn administer the test to their customers (i.e., the individual test takers). Thus, the testing organization, who is the owner of the test, is not the controlling entity that makes the decisions about the collection and use of the personal information of its customers/clients/consumers. In these instances, the testing organization becomes a processor/service provider (e.g., for test scoring, for record-keeping) to

[21] The language of AB 25, amending the CCPA, also applies to job applicants, as well as candidates for officer and board positions. The ATP submits that the final regulations must cover all affected individuals.

the entity that actually controls the privacy decisions[22] — and whose privacy policy governs the notices to consumers. Consequently, a testing organization will have contact information on a number of representatives of controlling business entities, which are outside of the scope of the CCPA at least for 2020. The ATP strongly encourages the Attorney General to include guidance on how a business should handle this information in the final regulations. When a business deals with another business, and a representative of the second business provides his or her contact information, for 2020 at least, that collection is not treated as the collection of personal information, but is "business information." For example, when such a business contact provides a business address, telephone number, and a business email address, the representative is acting on behalf of his or her employer – the person is not the "consumer" and the business is not "a natural person" as defined Section 17014 of Title 18 of the California Code of Regulations. *See* Cal. Civ. Code §1798.140(g).

In addressing this issue in the final regulations (and beyond 2020), the ATP submits that the Attorney General should consider the interpretation of similar language adopted by the Office of the Privacy Commissioner of Canada under the Personal Information Protection and Electronic Documents Act ("PIPEDA"), *Bulletin on Personal Information* (2013). Essentially, that bulletin holds that PIPEDA does not apply to an organization in respect of the business contact information of an individual that the organization collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession. Even so, the bulletin does note that some contact information (e.g., personal cell phone number) may still be considered personal. Indeed, the ATP notes that the Ontario bulletin improperly fails to recognize that a self-employed individual is sometimes a business and at other times, the person will provide personal information – in our opinion, a business should be allowed to make this distinction when it has sufficient evidence to determine that an individual has provided business contact information as part of a business relationship.

In the context of privacy notices for customers (e.g., of testing organizations) the requirements in the Proposed Regulations ("do not sell" and website privacy links) would be inapplicable at this time; the final regulations should reflect the exemptions or explain how the moratorium should be implemented for 2020.

3. Issues related to privacy policies.

As a general rule, a testing organization will use its privacy policy to provide the information required to meet applicable privacy laws and regulations. As the ATP discussed earlier, that fact makes it particularly important for the final regulations to recognize that, when

---

[22] Because the testing organization is providing processing services as a service provider, it may end up with test takers' personal information shared with it by the controlling entity. As discussed in Section 7 (*infra.* at pp. 18-20), in the role as a service provider, the testing organization must adhere to the contractual obligations to protect the privacy rights of those customers' end users. *See also* General Overview – Roles and Responsibilities (*supra..*, pp. 3-4).

an entity documents that it is doing business in multiple states (or countries), the Attorney General should be required to take that fact into account in making any legal evaluation of the business's privacy policy.

In general, a business's privacy policy is intended to set forth a clear statement about what personal information is collected and how it will be used, as well as to set forth in a transparent manner what rights a consumer has with respect to that information and how the consumer may go about exercising those rights. In order to comply with the Proposed Regulations, privacy policies must be expanded to cover other matters, including handling requests from consumers, dealing with collection of personal information of minors, and adding information related to "Do Not Sell" and opt-out opportunities. Accordingly, the ATP recommends that the final regulations clarify that a business shall be allowed to provide information about, and access to, the "Do Not Sell" link and/or the opportunity for the consumer to opt out of the collection and use of personal information, in its privacy policy.

Despite the statement in the Proposed Regulations that, "The privacy policy shall not contain specific pieces of personal information about individual consumers and need not be personalized for each consumer[.]" (§308(a)(1)), the Proposed Regulations apparently contemplate that a business will be required to make significant changes to its privacy policy regarding the "look back" period, to address: (1) the categories of personal information collected within the preceding 12 months (and categories of sources); (2) whether the business has sold/disclosed certain personal information within the preceding 12 months to third parties for a business or commercial purpose; (3) the categories of personal information covered; and (4) if the business sells personal information of minors under age 16 without parental authorization. *See* §999.313(1)(E). The ATP believes that such "backwards-looking" information will be unique for different consumers and for different situations; thus a privacy policy should be written to notify consumers about its "future" intentions, as opposed to what may have taken place in the past twelve months. This approach seems especially appropriate given the changes that are likely to occur in the way future privacy policies are structured and the details they contain. Quite clearly, the "look back" feature of the CCPA is most appropriate in responses to specific consumer requests, to provide the specifics of what actually was collected and how it was used. Accordingly, the ATP recommends that the Attorney General clarify that the language in §308(a)(1) should be followed and any "look back" information should not have to be communicated in the privacy policy itself.

A further requirement in §999.308(1)(B) is that the business must, "Describe the process the business will use to verify the consumer request, including any information the consumer must provide." As discussed in Section 4 (*infra.* at pp. 15-17), the required methods and procedures for how a business must handle request verifications are complex and will make it difficult to come up with an accurate uniform description in "plain, straightforward language"

and to avoid the use of "technical or legal jargon." The final regulations should clarify that the business must provide a "reasonable" description of its procedures.

Another issue that arises today in privacy policies of many testing organizations is the identified use of personal information for research purposes (e.g., to update test norms such as statistical means and standard deviation, conduct item or test fairness analyses). The ATP notes that such research generally uses anonymous test taker information, such as test results based only on gender or other demographics (e.g., age, country). Similarly, in order to comply with federal and state anti-discrimination laws, employers often require testing organizations (as service providers) to keep anonymous aggregated data about the number of job applicants in special populations – the same types of information are commonly kept by employers to protect against discrimination claims. [23]

The CCPA makes it clear that a business is free to collect, use, retain, sell, or disclose consumer information that is de-identified or aggregated. *See* Cal. Civ. Code §1798.140(o)(2). The ATP submits it would be helpful for the final regulations specifically to provide examples explaining appropriate uses of such information, including uses in testing, where anonymous personal information has been de-identified and is then aggregated so that no information identified to the consumers is shared or disclosed. Most often, testing organizations include disclosure of such research uses of some personal information on an anonymous and aggregated basis in the test taker agreement, so that they do not have to go back to test takers a second time with a new notice.

4. **Issues concerning verification of requests.**

In order to respond to requests to know and to delete personal information collected by a business, the Proposed Regulations require different verification procedures based on whether or not the consumer exercising the right maintains a password-protected account with the

---

[23] These considerations also impact what information a privacy policy discloses on the retention of personal information. If the business has documented needs for specific personal information to comply with federal/state laws, or must provide personal information to a customer for its legal purposes, then the business will be forced to deny requests to delete that personal information. Similarly, test takers usually expect that their test results/scores will be available for as long as they are needed by the actual customer (e.g., employer for as long as it is seeking to fill a job, certification body for as long as a person is seeking certification, consumer for as long as the results have meaning), so retention of test results for many months is quite common.

business.[24] When the testing organization uses a password-protected account, the verification required under the Proposed Regulations should be satisfied using the same technology available to enable the business to match the consumer to the account, just as the system enables that consumer to change his/her password; nothing more should be required. *See* §999.313(c)(4). The consumer presumably is starting this process armed with the account information s/he already possesses, and the business will be able to match that information directly to the consumer. Requiring a business to go back to the requester for "re-authentication" is simply redundant and creates an unnecessary burden on the business.

Verification methods that should be required for a non-password account or non-account request ought to focus appropriately on the level of fact-based analysis by the business – to verify the individual's identity to a "reasonable degree of certainty" if he or she is seeking access to certain categories of personal information or to a "reasonably high degree of certainty" if he or she is seeking access to specific pieces of personal information the business collected. If an individual is requesting the deletion of personal information, the business must verify the identity to a reasonable degree or reasonably high degree of certainty, depending on the sensitivity of the personal information and the risk of harm posed to an individual by an unauthorized disclosure.[25]

---

[24] For these requests, the Proposed Regulations require "at a minimum" that the business provide consumers with a toll-free telephone number. *See* §999.312(a) and (b). The ATP submits that this requirement is singularly inappropriate. Someone from the business has to transcribe the information (in real time or from audio), which is likely to result in data entry errors and failure to understand what the consumer has said/meant, either of which could result in potential liability for the business. The most accurate way for the consumer to provide request information, including verification information, and for the business to receive it without error, is for the consumer to fill out an electronic or paper form. Audio recording of this information also may result in technical problems, resulting in lost information. Finally, having an audio recording of this information presents an added exposure for the business.

[25] For a request from a consumer that has no account with the business, the Proposed Regulations state that the business must verify the request with a reasonably high degree of certainty. "A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request." *See* §999.325(c). The ATP submits that this approach represents an unwarranted burden on a testing organization unless the requester has presented documentation from which the testing organization can determine that there is a reasonable likelihood that the consumer in fact took a test with the testing organization (e.g., the name of the test, the date it was taken, the place it was taken) or offered an explanation as to why the requester believes the testing organization has the consumer's personal information, which evidence may include a statement to that effect in the attestation. Absent such a *prima facie* showing, there is no reason to believe that a [FOOTNOTE CONTINEUD ON NEXT PAGE]

To a great extent, the differences in the level of verification are based on the business having to conduct a risk analysis of the sensitivity of the personal information and the likelihood that someone other than an actual consumer would attempt to gain access to (or seek to cause harm by deleting) a consumer's information. *See* §999.323(b)(3). It bears repeating that most testing organizations are not generally in the business of conducting marketing/advertising operations based on the use of consumers' personal information; thus, the only basis upon which a consumer should need to make a request is if s/he previously had taken a test from or through the testing organization. Here again, then, we submit that the requester must be able to first demonstrate that s/he has (within the past 12 months) had a relationship with the testing organization that would warrant the business undertaking the verification attempt. Such a requirement is also consistent with the Proposed Regulations language that one factor the business should address is, "Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated." The ability of the requester to provide sufficient information about his/her testing event gives the testing organization the most relevant piece of information from which to verify the request.

The ATP also has a grave concern about the validity of the Proposed Regulation (§999.313(d)(1)) that, when a requester for deletion cannot be verified, the request must be treated as one to opt-out of the sale of personal information. Initially, this requirement is predicated on a false assumption that a business even possesses personal information to begin with, compounded by the mistaken assertion that the business automatically is engaged in selling it. Indeed, if a business actually has determined it possesses any personal information about the requester, except for the apparent lack of verification, there would be no absolutely no reason not to respond, even if a denial is required. The business should not be penalized for the failure of the requester to adequately verify himself/herself. In the context of a testing organization, the ATP once again reiterates its view that any valid request (either for access or deletion) must include evidence from the requester that identifies the test s/he took and the location and date of the test administration. Plus, denial may be required by an excpetion (e.g., the IP rights of the testing organization). Finally, as noted previously, the requester's test results/scores may be owned by someone other than the requester, and thus, the requester may not have the actual authority to delete the information.

Equally important, the ATP objects strenuously to the requirement that a business permit consumers to make requests through an "agent." The Proposed Regulations requires a business to "explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf." *See* 999.308(b)(5). We strongly believe that the covered business must not be charged with the legal responsibility to tell consumers how they can

---

testing organization would have any personal information on that individual. Spurious requests from consumers who cannot provide specific information about their testing event can only lead to unjustified regulatory burdens being placed on these businesses. *See, also,* fn 26 at p.17.

designate an agent – such responsibility must rest totally with the consumer according to standard legal rules of agency. Similarly, it makes no sense for the Attorney General to establish a procedure for a consumer to abdicate his/her direct relationship with a business in order to pursue his/her rights under the CCPA. Not only does this put an unrelated third party (who has no knowledge about the relationship) into the middle of the issue, but it is particularly troublesome when it comes to verification of the identity of the consumer; when a business cannot get direct access to the consumer to provide additional information, it adds serious complications to the process of a business's legitimate attempt to make the verification.[26] If the business needs more information which the agent does not have, the agent presumably then has to go back to the consumer, thereby adding unnecessary time and expense to the process. And equally burdensome, the business has to "verify" that the agent actually has authority to represent the consumer, another additional step to the process. It seems to the ATP that if protecting a consumer's personal information is important to the individual, the person should handle a request on his or her own, rather than sharing that personal information with yet another entity.

Finally, the Proposed Regulations impose an affirmative obligation on a covered business that is not found in the CCPA: "A business shall implement reasonable security measures to detect fraudulent identity verification activity and prevent the unauthorized access to or deletion of a consumer's personal information." *See* §999.323(d); *see, also,* §999.313(c)(6). Although the Proposed Regulations do not define what it means to implement "reasonable security measures," the ATP recommends that the final regulations should adopt a definition based on the Cybersecurity Framework (CSF) developed by the US National Institute of Standards and Technology ("NIST"), as well as public voluntary standards in the ISO 27000 family of information technology management standards, or a similar information security framework. The NIST CSF functions to "aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and

---

[26] An "agent" is unlikely to have any information about the testing event, which makes it impossible for the agent to provide the key fundamental information the ATP has proposed should be required as part of the verification. The Proposed Regulations set up opportunities for spurious agent requests. As one ATP Member has informed us, "we've started getting requests from an organization called "deseat.me" that seems to have us in their list of suppliers. Typically these requests are for people about whom we have no knowledge and the only information we get is an email address. And it's unclear whether the request has authority. As such, we are forced to waste a lot of time and energy trying to track down these phantom test takers." If a consumer has a legitimate reason to require an "agent" to administer his/her affairs, a legal option is already available through a power of attorney.

improving by learning from previous activities."[27] Under the CSF, a business's security plan focuses on five basic functions: (1) identifying critical infrastructure and data; (2) protecting your data; (3) detecting potential cybersecurity events; (4) responding to detected events; and (5) recovering capabilities and/or services that were impacted by a cybersecurity event. As a voluntary standard, the CSF also builds on other public voluntary standards, such as ISO/IEC 27000 *et. seq.* (2018), entitled "Information technology — Security techniques — Information security management systems — Overview and vocabulary."[28] The ATP also recommends citing the ISO standards as part of a definition for the term "reasonable security measures." The ATP contends that aligning the CCPA with these voluntary standards-based security measures will enable covered businesses to adopt security approaches that will be consistent across different states/countries. Accordingly, references to both the NIST CSF and the ISO standards should be included in the final regulations. Continued reliance by the Attorney General's Office on the checklist of twenty controls defined by the Center for Internet Security previously announced in 2016 as the "minimum level of information security" (*see 2016 Data Breach Report* (Feb. 16, 2016)), should be expanded. The ATP contends that the mere identification of controls does not provide as much value to a business as concrete steps to deal with data protection.

For example, ISO 27001 provides a management system framework of documents, policies, procedures, and controls that enables an organization to systematically evaluate risks to the confidentiality, integrity and availability of its information and put in place appropriate measures to address the risks and follow other requirements of the standard. A key focus is that the standard requires continual improvement over time. Although organizations are free to select security controls based on an evaluation of their own risks, in general there are 114 controls specified in the standard (compared to 20 specified in the 2016 Report).

Related to the needed definition of "reasonable security measures," the ATP also recommends that the Attorney General should adopt a "safe harbor" provision in the final regulations stating that, if a business uses standardized commercial encryption techniques to protect consumers' personal information while they are stored and for transmission to the

---

[27] The Cybersecurity Framework was developed in response to Executive Order 13636, which was directed to critical national infrastructure. Nevertheless, the CSF serves as a useful guide for any business to enhance its information security program. Current version 1.1 was released by NIST on April 16, 2018; version 2.0 is under development. Additionally, NIST is developing a "privacy framework" that is expected to be published in 2020.

[28] The ISO 27000 family of standards for information security management systems (ISMS) includes ISO 27001 (an audit/certification requirements framework by which a business may respond to information security risks, compliance, and regulatory requirements). ISO 27002 contains voluntary best practices. A new standard that extends both ISO 27001 and ISO 27002 is ISO 27701 (2019), which specifies requirements and provides guidance for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS).

consumer in response to a verified request, that action shall protect the business from any security violations of the CCPA. While "reasonable security measures" do not automatically include the use of encryption, if a business decides to encrypt personal information in its systems (and for communicating personal information back to a consumer), that action will greatly enhance the level of protection afforded such data. A number of different encryption algorithms are used today for a variety of commercial purposes.[29] The final regulations should permit a business to select a commercially-available and industry-accepted encryption algorithm based on its own needs and purposes, and so long as the business encrypts all consumer personal information it collects and uses, the safe harbor should apply.

This "safe harbor" is completely justified inasmuch as the CCPA expressly allows consumers to sue businesses when their "nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information." *See* Cal. Civ. Code §1798.150(a)(1). Clearly, the Legislature itself has focused on when "nonencryped" data is at risk.[30] Accordingly, if a business has encrypted consumers' personal information, it has taken an affirmative action to remove the risk of unauthorized access and disclosure – even if some personal information were illegally obtained, it cannot be used. In recognition of this, the final regulations must be clarified so that a business is not subject to substantial statutory penalties (of between $100 and $750 per incident).

5. **Issues concerning responses to requests.**

When a business cannot verify the identity of a requester, the Proposed Regulations require it to "provide or direct the consumer to its general business practices … in its privacy policy." *See* §999.313(c)(2). This response is redundant, inasmuch as the requester obviously already has access to the privacy policy and all other notice information made available by the business in order to make the request. Therefore, this Proposed Regulation represents yet another instance of unnecessary burdens being placed on the business; it should be deleted.

---

[29] One such algorithm is the Advanced Encryption Standard (AES) used to encrypt and decrypt electronic information, which was approved for use by the federal government in November 2001 and has since been widely adopted by private industry. Today, AES protects everything from classified data and bank transactions to online shopping and social media apps.

[30] The ATP submits such a "safe harbor" is intended at a minimum to cover all liability for a security breach – if a business suffers a breach and all personal information is properly encrypted, none of the personal information is actually exposed. Moreover, the "safe harbor" also should apply to both to the "reasonable security measures" requirements in §999.313(c)(6) and §999.323(d).

In our view, the more important aspects of how a business must respond to requests focus on several specific provisions related to denials of requests. Beyond the clear statement (§999.313(c)(4)) that a business shall not provide key sensitive information (i.e., SSN, driver's license, financial account numbers, account password), the Proposed Regulations also state that the business "shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks." *See* §999.313(c)(3).[31] The ATP supports this approach and submits that it provides a business with appropriate flexibility to examine all potential impacts of a request for access. *See* Section 4, *supra.,* at pp. 15-17. Because this provision has broad application throughout a covered business's operations, it would be helpful to have the final regulations include use cases to provide further guidance. For example, a request in a testing setting could involve information that would comprise the security of the requester's test information as well as the business's testing system and/or its test products directly. In such a situation, it would be appropriate for the testing organization to deny access.

Similarly, the Proposed Regulations expressly allow the business to deny a request where disclosure would "conflict with federal or state law." *See* §999.313(c)(5). As the ATP previously discussed (*supra.* at p. 4), secure tests and other test materials often are proprietary intellectual property ("IP") of the testing organization (i.e., test items, test manuals, scoring software, test delivery platforms), which the business must protect against disclosure in order to maintain test security and prevent cheating on the test. Thus, if a request for access to a test taker's personal information involves any actual disclosure of the testing organization's IP, the test taker would not be entitled to access such IP and the business will screen out all such IP from what is made available to test taker.[32] Although we submit that federal patent, trademark, copyright, and trade secret rights are easily understood as potential "conflicts" with a consumer's right to access, the Proposed Regulations fail to provide any explicit guidance in this area. To avoid confusion on this important point, the ATP recommends that the final regulations should provide details for how a business is permitted to deny some or all of a request when its federal IP rights conflict with the consumer's right to access.[33] *See* discussion of the impact of a testing organization's IP, *supra.* at pp. 2-3.

---

[31] Indeed, the Proposed Regulations allow that if a business maintains consumer information that is de-identified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request. §999.323(c)

[32] The protection of the testing organization's IP is also consistent with the usual terms contained in the test taker agreement, so every test taker will have been put on notice about this restricted access. As discussed in fn 6, *supra,* test results/scores are likely to be considered by the testing organization to be at least in part covered IP, which will result in denial/partial denial of requests that would entail disclosure of the testing organization's IP,

[33] Except in the case of trade secrets, a business that owns other IP assets will have evidence of those rights issued by the respective governmental body. The final regulations should merely require the business to provide that publically available information to justify its denial of the request.

Finally, denial of requests to delete personal information requires the use of a "two-step" confirmation process as set forth in §999.312(d). The ATP objects to such a process as completely unnecessary. Where no exceptions exist, the requirement is predicated on what can only be described as a "paternalistic" assumption that a consumer does not really understand what s/he is requesting and then places an obligation on the business to essentially double-check whether the consumer really intends to have his/her personal information deleted. In situations where exceptions apply, the ATP suggests that a business will be communicating with a consumer in fully dealing with a denial so any confirmation step is accomplished as part of the denial process. In either case, the burden on the business is exacerbated if an agent is involved. If the consumer elects to request deletion, regardless of how the business verifies the request, there is no need for any confirmatory step. The final regulations should clarify these points.

On a related issue, the Proposed Regulations also require that consumer access responses should be made portable provided technically feasible. *See* §999.313(c)(7). The ATP has several concerns about this language. First, no single standardized or uniform format for interchanging test data exists, so there is no "technically feasible" way to enable a consumer to port test results/scores. But more fundamentally, test takers do not "comparison shop" among testing organizations for a given test, and a high stakes test for a certain purpose is typically only offered by a specific test owner. Thus, a consumer's right to "portability" – to take personal information from one business and send it to another testing organization –is practically meaningless. Such portability poses a business challenge, as well as a technical challenge, for organizations that develop or deliver tests, considering the issues of test security, possible conflicts of interest and protection of intellectual property. Thus, the ATP submits that a testing organization would be within its rights to deny a request for test results/scores by arguing that: (1) data portability is not technically feasible; (2) its company assets (e.g., intellectual property rights) must be protected: and (3) the rights of an entity that is paying for the individual test taker's assessment (e.g., employer) or a test copyright holder (e.g., test author) must be protected.

6. **Issues concerning time to respond to requests.**

For the requests to know and to delete, a business must acknowledge receipt within 10 days, providing additional information about how the business will process the request. A business must respond within the 45-day deadline set forth in the CCPA (with an additional 45-day extension if the business gives notice to the consumer); the Proposed Regulations clarify that the timeline begins to run upon receipt of the request, "regardless of time required to verify the request." Given this already compressed timeline, the ATP recommends that the final regulations drop the required acknowledgement – the business has enough to do to begin the verification process and prepare a response within the 45-day period. Moreover, since the consumer will receive a substantive response in most instances within the 45-day period (or a notice of the extension), the value of an acknowledgement is questionable.

7. Issues with respect to the use of "Service Providers".

The ATP generally endorses the Proposed Regulations concerning the definition of "service providers" (*see* §999.314). However, the Proposed Regulations do not go nearly far enough in identifying the scope of how many service providers operate. This is especially true in the testing industry, where a testing organization that is not directly selling testing services to consumers and has a contractual relationship with the controller automatically should be deemed to be a "service provider." As such, when a business provides various testing services to or on behalf of the organization that actually owns the test and collects the personal information of consumers, such a business functions as a "service provider." The Proposed Regulations seem to accept this position by providing: "To the extent that a business directs a person or entity to collect personal information directly from a consumer on the business's behalf, and would otherwise meet all other requirements of a "service provider" under Civil Code section 1798.140(v), that person or entity shall be deemed a service provider for purposes of the CCPA and these regulations." *See* §999.314(b).

However, the Proposed Regulations are not consistent with the CCPA on several key points. Accordingly, in order to eliminate any confusion, the ATP contends the Attorney General should make changes in the final regulations to fix those discrepancies.

Critically, while the CCPA indicates that a service provider need not reply to consumers' rights requests, the Proposed Regulations state that "a service provider must provide the specific basis for denying requests from consumers regarding their personal information collected or maintained by the service provider on behalf of the business." *See* §999.314(d). Yet, the same section of the Proposed Regulations also would require that a service provider direct consumers to submit their requests to the relevant business and to provide the consumer with the contact information for that business "when feasible."[34] Equally confusing, the Proposed Regulations also attempt to clarify that an entity can be a service provider to the extent it collects personal information from consumers as directed by a business as well as where the service provider acts on behalf of another entity that is not a "business" under the CCPA, provided the entity

---

[34] For example, it is common for a testing service organization to provide online software which can be used to deliver to, and score tests for, California consumers. Such an organization is a service provider to test publishers, test sponsoring organizations, or employers. When a consumer requests information from the service provider, it would be inappropriate for the service provider to share that information, but instead it should pass the request to the testing organization that controls the testing event, including making the decisions about the collection and use of personal information. This result is required partly because the service provider may not be able to identify the consumer and partly because the consumer has a contractual relationship with the controlling business, not the service provider. The final regulations should be modified to make this relationship sufficiently clear.

otherwise meets the requirements for a service provider. *See* §999.314(a) and (b).[35]

Unfortunately, these Proposed Regulations create more doubt and confusion than they achieve clarity in this area. Because of this confusion, the ATP is concerned that testing organizations that are engaged in a variety of services, often performed for owners of tests and testing programs, will be viewed by consumers – and thus, by the Attorney General – as having the primary relationship with a consumer and therefore, be deemed to be the controlling business. This confusion is likely to go unresolved because the Proposed Regulations do not adequately take into account the contractual relationships that exist with a variety of service providers (e.g., test delivery, test scoring, test security) (*see supra.* at 3-5).[36] As we noted, it would be useful for the final regulations to adopt (or adapt) the definitions from the GDPR for the entity that determines what personal information is collected and how it is used (i.e., the "controller") and the entity that follows the instructions of the controller in processing personal information on the controllers behalf, even if that entity may be collecting the information directly from consumers. Absent this clarification, the ATP is concerned that the primary responsibilities for compliance with the CCPA may improperly be shifted away from the controlling business to service providers/processers.

Finally, the Proposed Regulations fail to provide any guidance on the requirements for a "data broker" that were added in the amendments from AB 1202. That amendment defined a data broker as a "business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship, subject to specified exceptions." In light of that amendment, and the potential for mistakenly requiring a testing organization liable to register as a "data broker," the ATP reiterates its previous comments about how a testing organization shares personal information, especially test takers'

---

[35] Compared to these inconsistent statements, we note the clarity surrounding the following point: "A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider." Despite the apparent straightforwardness of this language, it is still inappropriately vague as to identifying the scope of roles a business may legitimately play as a service provider. The final regulations should provide additional clarity acknowledging the broad scope of services related to an underlying business agreement that should be allowed.

[36] The Proposed Regulations clarify that a service provider may "combine personal information received from one or more entities … to detect data security incidents, or protect against fraudulent or illegal activity. That language perfectly fits the business operations of some testing organizations that provide test security services.

test results/scores with its partners and service providers in order to fulfill its responsibilities to the consumer (*see supra.* at pp. 3-4 and 12-14). In other circumstances, where the third parties involved in the provision of the overall testing services may not have a "direct relationship" with the test takers, that does not make the controlling business a "data broker." Nor is the third party a "data broker" by virtue of collecting personal information on behalf of the testing organization. First, neither the testing organization nor the third party service provider is not selling or disclosing test taker information for any marketing purpose, but are merely sharing information necessary to enable the other business(es) to complete its portion of the testing services for the specific consumer. Second, both the underlying testing organization and any service providers/partners are part of the "common interest" group providing the testing services to the consumer, so a "direct relationship" should be inferred to exist for each entity engaged in the process.

8. Issues with recordkeeping

The Proposed Regulations require that a business keep records for at least 24 months and include the following information: request data, nature of request, manner of submission and basis for any denial. §999.317(b).[37] In addition, businesses that "alone or in combination" (a phrase that is undefined and unclear) receive or share records of 4 million or more California residents would be required to compile detailed metrics on the value of different requests under the statute and median number of days to respond to each, as well as any signed declarations obtained from consumers as part of the consumer verification process.[38] §999.317(g).

The Proposed Regulations require a business to post this information as part of its privacy policy – or provide a link to the information from its privacy policy. §999.317(g)(2). This approach represents a novel requirement in U.S. privacy law, and represents an overly-

---

[37] Separately, the Proposed Regulations require that a business provide adequate training for employees on "all of the requirements in the regulations." *See* §999.3179(a). The ATP supports this mandate in the context of enabling a testing organization to deal with the CCPA along with other state/country-specific laws/regulations in the United States, as well as foreign laws and regulations (e.g., GDPR).

[38] We note that the determination as to whether a business has 4 million records suffers from the same problem as for the 50,000 California consumers eligibility requirement – it is often difficult or even impossible to know the residence of some test takers. *See* Comment Section 1, *supra.* at p. 8. As such, the eligibility test for requiring these metrics is unreasonably vague. Moreover, the purpose seems to be more predicated on enforcing the CCPA than to producing any benefit for California consumers. Furthermore, we see no relationship between the number of requests a business may experience to any level of lack of compliance under the CCPA or equally, to any bad reputation a businesses may seem to acquire due to the number of requests it receives.

burdensome and costly mandate for each business to comply.[39] When those costs are compared with the largely illusory benefits to consumers of having access to such metrics, the ATP fails to understand what relevance a 2-year record of requests/outcomes has to the business's ability to protect consumer personal information, or even to adopt reasonable procedures for handling consumer requests. Instead, this requirement seems aimed more to giving the Attorney General CCPA enforcement information to use during an enforcement investigation. As such, the ATP submits that the final regulations should drop the requirement to provide this information directly or indirectly through a business's privacy policy.

Especially if the objective is to require the business to retain enforcement related data, it is very troubling that apparently a business may not use its own data for any purpose beyond this reporting. §999.317(c). In reality, a business needs to be able to access all such information about its handling of all consumer requests specifically for the purpose of documenting what it did if the same consumer comes back to the business to complain about what was done/nor done. If the business does not have legitimate access and use to its own business records, it will be unable to document the previous actions taken under the regulations. Accordingly, the ATP recommends that the Proposed Regulations be modified to clarify that a business may use its records as part of its procedures for handling requests and to evaluate and modify its processes.

10. <u>Issues with enforcement</u>.

The ATP is very concerned about how its Members can be in a position to comply fully with whatever final regulations are published, especially inasmuch as it seems highly unlikely that the regulations will not be finalized until the Spring of 2020, which will be only a few months before the presumed July 1 enforcement date. As mentioned earlier, many ATP Members have been adjusting their privacy policies over the past two years, first because of the GDPR, and now because of the CCPA. Nevertheless, until final regulations are published, there are uncertainties in how some issues will ultimately be resolved.

The initial cost of compliance with the CCPA for each business has been estimated at between $50,000 and $2 million (or more), depending on the size of the business. Accordingly, ATP Members are likely to rely on their existing data privacy and information security policies until the final regulations are announced. But even that level of uncertainty pales in comparison to the press conference statement by the Attorney General on October 10, 2019, which seemed to indicate he might take enforcement actions for noncompliance between January 1 and July 1, 2020. For obvious reasons, the ATP strongly urges the Attorney General to forestall any enforcement until businesses have seen and can understand the full requirements of the final regulations and can have a reasonable opportunity to finalize their compliance plans. In our

---

[39] To the best of the ATP's knowledge, the GDPR does not require such publication, nor does the new privacy law in India. This requirement is overly burdensome and will cause a testing organization to expend resources to comply that would be better used for protecting the privacy of personal information.

opinion, a six-month delay in enforcement, until January 1, 2021, would make sense. We believe this recommendation is appropriate, because with the 12-month "look-back" period, such an enforcement action commenced on that date would fully enable the Attorney General to take into account all aspects of a business's compliance after the statutory effective date of January 1, 2020.

CONCLUSION

On behalf of the international testing industry, the ATP has provided comments on the Proposed Regulations for implementing the CCPA. We have articulated a number of unique circumstances that are common in the testing industry. We have indicated that many testing organizations are smaller/medium-sized businesses. Together, we believe these reasons justify modification of the Proposed Regulations when balanced against the rights of individual test takers as consumers.

Among the significant positions set forth in these comments are the following recommendations:

- The final regulations must clarify the definition of "sale" to avoid application of overly-prescriptive privacy requirements to situations where the sharing of an individual's test results/scores with service providers of the testing organization, which would defeat the very purpose the consumer has in taking the test in the first place.
- The final regulations must clarify the broad scope of services provided by a "service provider" that are completely related to the underlying contract with the covered business, especially in the testing industry where a variety of component testing services are necessary to the accomplish the underlying contract with a consumer for testing services.
- The final regulations must clarify that test results/scores are not to be treated as "personal information."
- The final regulations must clarify that the intended purpose of the CCPA is to limit the sale, use, and distribution of personal information for commercial marketing/advertising purposes.
- The final regulations must remove and/or reduce the incredibly complex, overly burdensome procedural requirements, which actually defeat the intended purpose of CCPA.
- The final regulations must clarify that the intent of the CCPA is to inform consumers of a business's privacy practices, regardless of whether the notice comes from the underlying contracting business or one of its service providers.
- The final regulations must not hamper a business's efforts to protect consumer privacy in a meaningful way or to divert resources away from data protection and compliance.
- The final regulations should more closely parallel those of GDPR, especially the definitions of, and distinctions between, data controller and data processor, in order to

maintain proper accountability for compliance with the organization that has the underlying substantive relationship with the consumer.

- The final regulations must highlight the distinction between inferences made about a person for marketing purposes, and those made in the process of providing testing services (i.e., analyzing and reporting test scores).
- The final regulations must clarify how to calculate the $25 million revenue and the 50,000 California consumer thresholds (as well as the 4 million consumers for the expanded metrics).
- The final regulations must require that a consumer provide request verification information about his/her relationship with a business, especially where a testing organization is involved (by providing information about the test that was taken, along with the date and place where the test was taken).
- The final regulations must establish an effective "safe harbor" for a business that encrypts consumers' personal information.
- The final regulations must remove the ability of a consumer to use an agent outside of a traditional Power of Attorney.
- The final regulations must delete and/or modify the record keeping requirements, which in themselves have no benefit to consumers, and to allow a business to use such information to improve its own compliance with the CCPA.
- The final regulations must address and provide guidance on how to handle employee (and job applicant) personal information and business contact information during 2020.
- The final regulations must be published and allowed to be implemented by covered businesses before any enforcement should occur.

Thank you for your attention to the important issues raised by the testing industry about the Proposed Regulations implementing the CCPA by affected members of the testing industry located within and outside of California. The ATP would be pleased to answer any questions the Attorney General's Office may have in response to these comments, including to do so in a face-to-face meeting. For any follow up, please contact our General Counsel at the number or email address shown below.

Sincerely,

ASSOCIATION OF TEST PUBLISHERS

William G. Harris, Ph.D.
CEO
601 Pennsylvania Ave., NW
South Bldg., Suite 900
Washington D.C. 20004

John Weiner, Incoming Chairman of the Board of Directors
Chief Science Officer
PSI Services LLC
611 N. Brand Blvd., 10th Flr.
Glendale CA 91203

Alan J. Thiemann
General Counsel
Law Office of Alan J. Thiemann
700 12th Street, NW, Suite 700
Washington, DC 2005
(202) 904-2467
ajthiemann@gmail.com