California: CCPA rights and obligations clearer following amendment bills and proposed regulations

The California State Governor, Gavin Newsom, signed into law, on 11 October 2019, six Amendment Bills (‘the Amendment Bills’) to the California Consumer Privacy Act (‘CCPA’). Assembly Bill (‘AB’) 25, AB 874, AB 1146, AB 1202, AB 1355 and AB 1564. In addition, the California Attorney General (‘AG’), Xavier Becerra, released, on 10 October 2019, proposed regulations (‘the Proposed Regulations’) to public comment. Alan L. Friel, Partner at Baker & Hostetler LLP, provides a detailed analysis of the CCPA’s revised consumer rights and business obligations following the Amendment Bills and the Proposed Regulations, and, in particular, provides advise on how businesses can start implementing a consumer rights request (‘CRR’) response process, finalising notices and otherwise preparing for the new year.

The CCPA, effective from 1 January 2020, will provide California consumers with new rights of transparency, choice, and control over their personal information. However, with dozens of proposed amendments under consideration and no draft regulations to flesh out the details of the new law, companies had been left to prepare without a full picture of what will be required. This is no longer the case, following the Amendment Bills and Proposed Regulations.

**What Consumer Rights Exist Under the CCPA?**
The CCPA grants California consumers several rights over their personal information, which is broadly defined and includes pseudonymous data like device IDs. A ‘consumer’ is a resident as defined by the California’s tax code, and thus is not limited to customers or consumers within the meaning of other California privacy laws.

The CCPA covers personal information collected in both business-to-business (‘B2B’) and business-to-consumer (‘B2C’) transactions. However, AB 25 delays application of the CCPA to current and former employees, job applicants and independent contractors until 1 January 2021, except for the obligation to give pre-collection notice under Section 1798.100(b) of the CCPA and the rights to sue following a data security incident under Section 1798.150 of the CCPA.

Similarly, AB 1355 exempts certain B2B data, specifically personal information in communications with a person acting on behalf of another business regarding providing or receiving products or services to or from such business, from most consumer rights, as well as pre-notice obligations, until 1 January 2021. However, this amendment does not include Section 1798.120 of the CCPA (the right to request to opt out (see below)) in the list of delayed provisions, but it does include Section 1798.135 of the CCPA (the do-not-sell business obligations), creating ambiguity in the application of the do-not-sell 'opt-out' for this type of personal information in 2020. Like AB 25, AB 1355 does not delay the private right of action for security incidents.

In particular, the CCPA provides that a California consumer has the right to request that a business:

- provide certain information about, and access to, the consumer’s personal information that the business is collecting, selling or disclosing (i.e. the right to request to know);
- stop selling the consumer’s personal to third parties (i.e. the right to request to opt out, otherwise known as a do-not-sell request); and
- delete the personal information that the business has collected from the consumer (i.e. the right to request to delete).

A business must provide notice to consumers of these rights by describing them in its general website privacy policy or in a section specific to California privacy rights.

Currently, more than a dozen states have put forth their own versions of the CCPA with variations on what is required, and more states are expected to follow this trend. However, so far, only Nevada has passed a new privacy law similar to the CCPA, and it appears unlikely that any other state will do so in 2019, as the legislative season is over or nearing completion in most states. The Nevada law is limited to a do-not-sell right for certain ‘covered information’ collected via an online service. The right is far more narrow than the California do-not-sell rights. The Nevada law became effective on 1 October 2019.

**How Does a Business Verify a CRR?**

Under the CCPA and the Proposed Regulations, verification requirements are targeted at verifying the identity of the requester, not the requester’s status as a California resident. Verification is required for consumer requests for information, access and copy, and deletion, but notably is not required for do-not-sell requests. Thus, for all but do-not-sell requests, a business must verify that the requesting party is the applicable data subject and must ‘establish, document, and comply with’ a ‘reasonable’ verification method, as described below.

The amended Section 1798.130 of the CCPA provides that ‘[t]he business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested.’ The Proposed Regulations provide that, in designing a reasonable method for verification, a business should consider factors such as the sensitivity of the data, the potential risk of harm
from unauthorised access and the manner in which the business interacts with consumers. As detailed below, businesses must follow different standards and procedures for verification depending on the type of consumer request and whether the requester is an accountholder.

### Accountholders

For consumers with password-protected accounts, verification may be achieved using the business's existing password authentication practices as long as those practices comply with general rules regarding verification and security. Before delivering the actual categories or specific pieces of consumer personal information or deleting the consumer's data, a business must take the additional step of reauthenticating the consumer's identity. However, if the business suspects unauthorised activity on the consumer's account, it must conduct further verification procedures or use the verification procedures for non-accountholders. Note that a business may not require the consumer to create an account in order to be verified.

### Consumers without accounts

For consumers without password-protected accounts, the Proposed Regulations require more stringent procedures and standards depending on the type of request, as detailed below.

#### Information Only

For information requests (i.e. information at the category level but not specific pieces of personal information), a business is required to ascertain to a ‘reasonable degree of certainty’ [emphasis added], which is to be understood as requiring a match of at least two data points provided by the consumer with those maintained by the business, that the requester is the applicable data subject.

#### Specific Pieces

For access and copy requests, a business must ascertain to a ‘reasonably high degree of certainty’ [emphasis added], which is to be understood as requiring a match between at least three data points and obtaining a signed declaration, under penalty of perjury, that the requester is the applicable data subject.

#### Deletion

For deletion requests, the required standard, either a reasonable or a reasonably high degree of certainty, depends on the sensitivity of the data and the risk of harm posed by unauthorised deletion. For example, the deletion of family photographs and documents may require a reasonably high degree of certainty, while the deletion of browsing history may require a reasonable degree of certainty.

### Verification Failures

If a business is unable to verify the requester's identity, it must respond to the consumer and explain why there is no reasonable method to verify the consumer request. A business has additional obligations depending on the type of request.

For verification failure of an access or copy request, a business must deny the request, refrain from disclosing any 'specific pieces' of consumer personal information, and evaluate the request as if it were an information request.
For verification failure of an information request, the business has discretion to deny the request. If the business chooses to deny the request, it must provide or direct the consumer to the section of its privacy policy setting forth its practices regarding the collection, maintenance and sale of personal information.

For verification failure of a deletion request, the business may also deny the request, in which case it must process the request as an opt-out. If the business is unable to verify the identity of any consumers in its database (for example, because the business does not collect enough pieces of identifying information), it must state so in the privacy policy.

**Authorised Agents**

Whether an accountholder or a non-accountholder, a consumer may designate an authorised agent to submit a request. In that instance, a business has discretion to require a verification of the agency relationship by requiring the consumer to either provide written permission to the agent or to verify his or her own identity directly with the business. If an authorised agent fails to submit proof of authorisation to act on the consumer's behalf, a business has discretion to deny the request. However, this verification is not required for authorised agents with power of attorney under the California Probate Code.

**Other Issues**

The CCPA and Proposed Regulations impose additional requirements and restrictions on the verification process. On an annual basis, the business must also evaluate the feasibility of establishing a reasonable method of verification and document this evaluation process.

If a business collects personal information from the consumer to verify a request, it may not use that information for any purpose other than verification of the request. Businesses should request additional information for verification purposes only when necessary, must use such information only for verification or security purposes, and must delete such information 'as soon as practical' thereafter. In particular, businesses should attempt to steer clear of collecting 'personal information,' 'medical information' and 'health insurance information' as those terms are defined in Section 1798.80 et seq. of Title 1.81 on Customer Records of the Civil Code.

Businesses must also implement reasonable security measures to detect unauthorised access attempts and for request responses. If a business maintains de-identified consumer information, it need not re-identify this information for purposes of verifying a consumer request, and it must not retain personal information longer than needed just to be able to respond to a future CRR. In addition, all notices and methods for exercising rights must be accessible to people with disabilities.

There are two notable omissions in the CCPA and current Proposed Regulations. First of all, there is no safe harbour for data security incidents where the verification requirements are met. Accordingly, if verification meets the regulatory standards but a request is nonetheless completed for the wrong individual, there is potential for liability. Therefore, to the extent that the Proposed Regulations permit discretion, it is recommended that more robust verification standards be utilised to avoid violating consumers’ privacy or risking a data security breach.

Secondly, there are no provisions regarding confirmation of California residency (in addition to verifying that the requesting party is the applicable data subject). While a business surely may provide non-residents with CCPA rights, the lack of any discussion of residency verification in the Proposed Regulations calls into question whether and to what extent a business may require residency verification.
How Does a Business Execute a CRR?

Upon receipt of a consumer’s request, a business should first verify that the individual making the request is the applicable data subject or an authorised party acting on behalf of the data subject. However, the CCPA does not specifically require verification for an opt-out request, and the Proposed Regulations specifically provide that verification is not required for an opt-out request, and further make opt-out the default for when a request to delete cannot be verified. However, an opt-out request may be rejected if a business has a documented, good-faith belief that it is fraudulent.

Once a business receives a CRR relating to information, access/copy or deletion, it must confirm receipt of the request within 10 days and provide information on ‘how the business will process the request,’ including a description of the verification process and the estimated time for further response. If the CRR is legitimate, the business must comply with any required disclosure or delivery within 45 days of receipt of the request. However, Section 1798.130(a)(2) of the CCPA provides that the 45-day period may be extended if reasonably necessary, for an aggregate response deadline of 90 days, provided that the consumer is given notice of the extension (i.e. up to an additional 45 days to verify a request that calls for disclosure or delivery).

There is an apparent conflict between the Proposed Regulations and the CCPA. Specifically, Section 999.313(b) of the Proposed Regulations states that any response period may be extended only by 45 days for an aggregate 90-day extension. On the other hand, the CCPA provides for an extension of up to 90 days beyond the initial 45-day verification period at Section 1798.145(g)(1). In the Initial Statement of Reasons ('ISOR'), the AG noted an apparent conflict between Section 1798.145(g)(1) of the CCPA (45 days plus up to 90 additional days) and Section 1798.130(a)(2) of the CCPA (45 days plus up to 45 additional days) and determined that the timing requirements in Section 1798.130(a)(2) of the CCPA should govern. However, unlike Section 1798.130(a)(2) of the CCPA, which applies only a reasonably necessary standard, Section 1798.145(g)(1) of the CCPA (now post-amendments Section 1798.145(j)(1)) applies to delays attributable to ‘the complexity and number of the requests.’ The AG seems to miss the distinction between the two different sections and their purposes for an extension. With respect to an opt-out request, a business must process the request ‘as soon as feasibly possible, but no later than 15 days’ from the date the request is received.

If the business does not act on the request of the consumer, the business must inform the consumer within the permitted time for responding that the business is refusing to honour the request, provide an explanation for the rejection, and disclose that the requester is entitled to appeal the decision. This clearly applies to all forms of consumer requests. There is no guidance in the CCPA or the Proposed Regulations regarding the appeal process. If a business is relying on an exception for not fully complying with a request, the business must disclose or delete the other information requested by the consumer, and which is not subject to exception(s).

Care should be taken not to suggest that the response is more complete than it is, as that could support a false advertising or deceptive or unfair business practices claim by the recipient, and potentially lead to a private right of action separate from a CCPA violation (enforcement of CCPA privacy requirements is limited to the AG). It should be noted that Section 1798.145(g)(3) of the CCPA permits a business to require a consumer to pay its reasonable costs for complying with the request or to refuse to honour a request to the extent that such response would be ‘manifestly unfounded or excessive,’ and that the Proposed Regulations confirm that such a charge is not a prohibited form of discrimination under the CCPA. When not all databases are searched, not all personal information is provided, or retention purposes or other deletion exceptions, it is recommended that this be explained and, when the search or disclosure was limited, consumers be given the right to pay for the burdensome additional response. Otherwise, responses must be cost-free.

What Types of Information Are Not Subject to a CRR?

Any information that does not fit the definition of personal information is not subject to a CRR. Therefore, a business does not have an obligation to comply with CRRs for information that is:

- 'publicly available,' which includes any information lawfully made available from federal, state or local government records, even if a business uses the information for a different purpose than that for which it was collected (AB 874 removes the purpose compatibility requirement);
- not reasonably capable of being linked, directly or indirectly, with a consumer or household (AB 874 adds ‘reasonably’ before ‘capable’), including de-identified information or aggregate consumer information; or
- a consumer's social security number, driver’s license number or other government-issued identification number, financial account number, any health insurance or medical identification number, account password, or security questions and answers (these data elements may not be disclosed ‘at any time’ in response to a right-to-know request).

In addition, AB 25 provides temporary exemption from all of the consumer rights provisions except for the pre-collection notice requirement for personal information from current or former employees, job applicants, and contractors if it is collected in the context of the consumer's employment status.

Furthermore, AB 1355 also provides a temporary exemption from all consumer rights provisions for personal information in communications with a person acting on behalf of another business regarding providing or receiving products or services to or from such business.

Note that both personal information exemptions under AB 25 and AB 1355 have a sunset date of 1 January 2021, unless the California State Legislature further amends the CCPA next year. Additionally, under both amendments, the consumers’ right to sue following a security incident is not delayed and still will commence on 1 January 2020.

**Other CRR Requirements and Exceptions**

A business cannot discriminate against a consumer because the consumer exercised any CCPA rights, subject to the ability to (1) offer different prices or qualities of service based on the value of the personal information; and (2) offer financial incentive programmes directly related to the value of the personal information. In the pre-amendment CCPA, the value is based on the value to the consumer, but AB 1355 changes that to the value to the business. Under the Proposed Regulations, a financial incentive initially offered for the collection of personal information, that is not later retracted when the consumer exercises CCPA rights, is not discriminatory.

The Proposed Regulations also provide multiple methods for determining the value of personal information. A business is not permitted to contractually require the waiver of CCPA rights, except to the extent that federal law preempts such restriction. This may limit certain waivers, releases and grants of rights in contracts even if good and valuable consideration is paid. However, the Federal Arbitration Act 1925 should preempt invalidation of class action waivers tied to arbitration.

Finally, the Proposed Regulations clarify the detail that must be applied to disclosures both in the privacy notice and in a CRR response. While Section 999.313(c) and (d) of the Proposed Regulations requires far greater granularity of disclosure than Section 999.308(b)(1)(d) does for the privacy notice, both require more specificity as relates to each category of applicable personal information than many had hoped. This will require revisiting data mapping and draft notices and response templates.

**Next Steps**
While many issues remain (for instance, how to treat cookies with regard to a opt-out request), there is now a lot more information on what the likely obligations will be for businesses come January 2020, and while keeping tabs on the rule-making process, businesses can start to prepare their privacy notices and develop a consumer rights verification and response programme.

Alan L. Friel  Partner
afriel@bakerlaw.com
Baker Hostetler LLP, Los Angeles

RELATED CONTENT

OPINION

Togo: Data protection law published in Official Gazette

OPINION

Interview with: Neal Cohen from Onfido

MEDIA

Dr. Christoph Bausewein, CIPP/E

NEWS POST

Serbia: Information security law published in Official Gazette

MEDIA

Laura Flannery, Assistant Commissioner at the Data Protection Commission, Ireland