Calif. AG Must Clarify Consumer Privacy Act Right Of Access

By **Seamus Duffy, Michael Stortz, Meredith Slawe and Julie Busta** (September 5, 2019)

Seamus Duffy

Michael Stortz

Meredith Slawe

Julie Busta

The California Consumer Privacy Act, set to become effective in January 2020, will introduce a powerful new set of rights for California consumers — broad and inalienable rights to control the sharing, disposition, retention and use of their data. The central premise of the new law is that all consumers have an inalienable right, rooted in Article I, Section 1 of the California Constitution, to reclaim and/or demand deletion of personal information from businesses covered by the new law.

That these rights are "inalienable" means that they can't be forfeited by waiver, or even by sale. Central to this new set of rights is the right of access — the right of a consumer to demand that a business disclose select information about data collected from the consumer, including the "specific pieces" of personal information collected from that consumer, in the year preceding the request. This right, in the overall context of the new statute as written, raises serious questions that the California attorney general should address in the regulations that are set to be proposed for comment later this year.

The Right of Access — Rules of the Road

Section 110 of the CCPA sets forth the new right of access, and Section 130 lays out the basic procedures for data access requests and responses.

Section 110(a) provides that a covered business must "disclose" to a consumer, in response to a verified data access request: (1) the "categories" of personal information collected about the consumer (i.e., name, Social Security number, web browsing history); (2) the "categories" of sources from which the information was collected (i.e., online order history, cookies, web beacons); (3) the business or commercial purpose for the collection or sale of personal information (i.e., fraud prevention, marketing, etc.); (4) the categories of third parties with whom the business shares personal information (i.e., tailored advertising partners, affiliates); and (5) the "specific pieces" of personal information it has collected about that consumer, all in the year preceding the request.

Section 130(a)(2) sets forth the base requirements for a data access response. The response must be provided free of charge within 45 days of receipt of the "verifiable consumer request"[1] through the customer's account with the business or electronically or in writing, at the consumer's election, if the consumer doesn't maintain an account with the business.

This period can be extended by an additional 45 days where "reasonably necessary," provided the consumer is given notice of the extension within the initial 45-day period, and perhaps also by an additional 90 days in some circumstances.[2] The information must be provided "in a readily useable format that allows the consumer to transmit this information to another entity without hindrance."[3]

The concept of a right of access to data may seem simple, but, as anyone who is ramping up for CCPA compliance in a large organization can tell you, it just isn't. There are at least three significant challenges that the California attorney general will need to meet and to resolve in the coming regulations to rationalize and make workable the right of access as drafted.

First, the regulations should make clear that businesses need not reidentify or link to a consumer previously deidentified or pseudonymized data in fulfilling a data access request. Second, the regulations should confirm that a business is required to provide only the personal information pertaining to the consumer verified as having made the request, and not data of other household members or shared device users. Finally, the attorney general should clarify that businesses are not required to forfeit trade secrets in responding to data access requests.

The Right of Access Should Not Require Reidentification of Consumer Data

The definition of "personal information" in the CCPA includes information that "is capable of being associated with" a particular consumer or household.[4] If this definition is read broadly to sweep within the concept of personal information data that has been deidentified or pseudonymized, then data access requests could trigger mass reidentification of previously deidentified or pseudonymized data, all to the detriment of consumers' broader data privacy interests.

Put simply, many businesses have made it a practice to protect consumer information by deidentifying or pseudonymizing consumer data, following best practices inspired by the privacy by design movement. A settled body of law in the United States and beyond recognizes that such data, because it can't be reasonably linked to a particular individual without additional information, isn't deserving of the protections of personal information.

The CCPA contains provisions to ensure that deidentified and psuedonymized data be maintained in such a way as to protect against reidentification.[5] In addition, the CCPA makes clear that the duty to provide access to personal information does not require a business to reidentify or otherwise link data that is not maintained as personal information.[6]

In order to fulfill the purposes of the CCPA, it is important that the attorney general address this tension created by the potential breadth of the statutory definition of personal information. The problem is that the definition of personal information, if read broadly, could sweep within the scope of personal information deidentified or pseudonymized data simply because such data "is capable of being associated" with the consumer, no matter how unlikely or remote the possibility of association might be.

If such a broad reading were accepted, the rights of access and deletion could then be read to require reidentification of such data for the purpose of fulfilling data access and deletion requests. This would be highly problematic, not only for the businesses who would be burdened with the obligation to reidentify data but also for the data privacy interests of consumers for whom the information was deidentified in the first place. The attorney general should make clear in the regulations that the rights of access and deletion in the CCPA do not require businesses to reidentify or otherwise link previously deidentified or pseudonymized data.

The Right of Access Should Be Limited to the Personal Information of the Verified

Requesting Consumer

A consumer has the right to access the personal information, including the "specific pieces" of personal information collected from that consumer in the year preceding the request. Under the CCPA, "'[p]ersonal information' means information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household."[7] The definition of personal information also includes "unique personal identifier," defined as "a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family."[8]

Again, the breadth of the definition of personal information in the CCPA presents a problem. Information associated with a "household" or a shared "device" will inevitably include highly sensitive personal information concerning particular data subjects sharing the household or device. Data access rights under the CCPA should not be interpreted to facilitate snooping by housemates and shared device users. No member of a household should be permitted to access sensitive personal information of others in the same household. Indeed, the CCPA includes a provision to ensure that "the rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.[9]

The California attorney general should make clear by regulation that the right of access is limited by the privacy rights of household members and shared device users. Businesses should not be required to provide access to or to delete personal information associated with a "household" or shared "device" without adequate assurance that the information is that of the verified requesting party, and no other.

The Right of Access Should Not Trump Intellectual Property Rights

The CCPA does not include express exceptions for the protection of intellectual property rights. Instead, the legislature deferred this issue to the regulatory process. The CCPA directs the California attorney general to address by regulation "exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights."[10] The attorney general should confirm by regulation that the CCPA does not trump or require the forfeiture of intellectual property rights.

Consider for example a data access request made by a loyalty club customer in the retail context.[11] It is one thing to say that such a customer is entitled to information on her own purchasing history. But should the retail business be required to deliver on demand to such a customer the entire customer relationship management profile of that customer, in "readily usable format" so that the customer can provide the profile to its competitors? Should the consumer be entitled to "access" to the design and format of the retailer's unique CRM system?

What if the request is made by a business which itself solicits data access request authorizations from consumers for the purpose of monetizing such data for a commission? "Customer information such as sales history and customer needs and preferences constitute trade secrets."[12] Indeed, customer preferences and related information is the most valuable and most carefully protected trade secret information in the retail industry. It is critical that the attorney general adopt proper protections for trade secrets and other intellectual property rights.

A Call for Clarity

The CCPA represents a tectonic shift in data privacy rights in America, and the California attorney general has an important responsibility to fill the gaps and address the ambiguities in the statute as written. Attorney General Xavier Becerra and his staff appear engaged and up to this difficult task. The issues identified here are but three of the fundamental issues associated with just one of the many new rights the CCPA creates. As the regulatory process moves forward, it will be critical for the attorney general to take practical and decisive action to make the CCPA a workable statute.

Seamus Duffy, Michael Stortz and Meredith Slawe are partners, and Julie Busta is an associate at Akin Gump Strauss Hauer & Feld LLP.

[1] A "[v]erifiable consumer request" is defined to include requests made by third parties on the consumer's behalf if the third party is registered with the Secretary of State to provide such services. See Cal. Civ. Code § 1798.140(y). The statute contemplates that the Attorney General will adopt regulations to guide businesses on appropriate standards for verification of consumer requests. See id. § 1798.185(a)(7).

[2] Section 145(g)(1) seems to permit still another extension by an additional 90 days "where necessary, taking into account the complexity and number of the requests," again so long as notice is provided to the consumer in the initial 45-day period. The Attorney General should clarify in the regulations whether the 90-day extension provided in Section 145(g)(1) is in addition to, or an alternative to, the 45-day extension permitted by Section 130(a)(2).

[3] Cal. Civ. Code § 1798.130(a)(2).

[4] Cal. Civ. Code § 1798.140(o)(1).

[5] See id. § 1798.140(h) (defining "[d]eidentified" to ensure against reidentification and to require safeguards to prohibit reidentification); id. § 1798.140(r) (defining "[p]seudonymize" similarly).

[6] See id. § 1798.110(d)(2) (access right does not require a business to reidentify data that is "not maintained in a manner that would be considered personal information."); id. § 1798.145(a)(i) ("This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.").

[7] Cal. Civ. Code § 1798.140(o)(1) (emphasis added).

[8] Id. § 1798.140(x) (emphasis added).

[9] Id. § 1798.145(j).

[10] Cal. Civ. Code § 1798.185(a)(3).

[11] An amendment to the CCPA to clarify that businesses can charge higher prices or provide a different level of service to a consumer based on the consumer's voluntary participation in the business's loyalty, rewards or discount program was passed by California's Assembly and is pending before its Senate. See AB 846 Customer loyalty programs, passed on May 28, 2019.

[12] Schein v. Cook, 191 F. Supp. 3d 1072, 1077 (N.D. Cal. 2016) (citing MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 521 (9th Cir. 1993)).