Baker McKenzie.

Memorandum

ATTORNEY-CLIENT PRIVILEGE
ATTORNEY WORK PRODUCT
CONFIDENTIAL DRAFT

Date: July 29, 2019

To: National Apartment Association

From: Michael Egan, Partner

Re: California Consumer Privacy Act Overview

We understand that the National Apartment Association ("**NAA**") seeks guidance about the requirements of the California Consumer Privacy Act ("**CCPA**")[1] and how the CCPA may apply to the operations of its members ("**Members**"). In general, CCPA establishes a broad range of data privacy obligations for covered businesses, including robust notice, opt-out choice, access, deletion, and related obligations. CCPA applies to "personal information" about "consumers" in California, which are broadly defined as any residents of California, and accordingly CCPA sweeps broadly to include consumers, employees[2], business partners, and other individuals who reside in the state.[3] CCPA primarily vests enforcement in the California Attorney General, where the enforcement authority includes injunctions and civil penalties of up to $7,500 per violation.[4] It also includes a private right of action, with statutory damages of up to $750 per consumer per incident, for situations involving unauthorized access to sensitive personal information within the meaning of California's existing breach notification and data security statute.[5] CCPA establishes broad authority for the Attorney General to issue regulations implementing CCPA's requirements, although such regulation is not expected to be issued in final form until perhaps Q1 or Q2 in 2020.[6] Absent federal pre-emption or amendments to the law in California, CCPA is set to become operative on January 1, 2020.[7]

---

[1] Cal. Civ. Code §§1798.100-1798.199.
[2] In its original form, proposed amendment Assembly Bill 25 aimed to redefine the definition of "consumers" to exclude a business's employee, contractor, or agent, whose personal information is used for purposes compatible with such a relationship. On July 11, 2019, a modified version of Assembly Bill 25 was passed out of the Senate Judiciary Committee. This modified version requires businesses to inform employees, contractors, or agents of what types of personal information they are collecting and their reasons for doing so. The modified Assembly Bill 25 also makes it clear that the private right of action applies to breaches of such employee personal information. Finally, the amended bill contains a one-year sunset period for the employee personal information exception.
[3] §1798.140(g).
[4] §1798.155(b).
[5] §1798.150.
[6] §1798.185.
[7] §1798.198.

Baker McKenzie.

I. JURISDICTION AND SCOPE

The CCPA primarily applies to "businesses," which are defined under the statute as for-profit entities doing business in the state of California, which directly or indirectly[8] collect personal information from California consumers, and meet one of the three thresholds below:

- Annual gross revenue greater than $25 million;
- Annually buy, sell, receive, or share the personal information of more than 50,000 consumers, households, or devices; or
- Derive 50% or more of its annual revenue from the sale of consumer personal information.

In addition to applying to businesses meeting the requirements above, the CCPA also applies to certain of their related entities, i.e., those entities that:

- control or are controlled by a "business" (as defined above); or
- share common branding with a "business" (as defined above) (e.g., shared name or trademark).

II. REQUIREMENTS

The CCPA's requirements relate to how businesses collect and disclose or transfer personal information of consumers. As noted above, the definition of "consumer" is not limited to traditional customers, but rather is defined as "a natural person who is a California resident."[9] "Personal information" is also broadly defined under the CCPA to include 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,"[10] which is arguably broader than the definition of "personal data" in the European General Data Protection Regulation (the "**GDPR**"), as the CCPA's definition of "personal information" includes information that relates to a household. The CCPA also provides specific categories of information in the definition of "personal information" that make clear that broad scope of what is included (e.g., browsing history or inferences drawn from other categories of personal information to create a profile about a consumer). However, "personal information" does not include publicly available information that is made available from federal, state, or local government records, subject to certain conditions.[11]

A. "Sale" of Personal Information and Opt-Out Choice

CCPA places prescriptive requirements on businesses that are engaged in the "sale" of personal information of consumers, including providing consumers special notice that it engages in the sale of personal information and a specific opt-out right for consumers who wish to opt-out of such sales. The challenge presented by these requirements is that "sale" is defined broadly to include "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 by the business to another business or a third party for monetary or other valuable

---

[8] A company may still be considered a "business" under CCPA when a third party collects California residents' personal information on behalf of the company, if the company (alone or jointly) determines the purposes of processing such personal information and how it is processed.

[9] §1798.140(g).

[10] §1798.140(o)(1).

[11] §1798.140(o)(2).

consideration."[12] That is, any transfer or disclosure of any personal information of a consumer to a third party for consideration, regardless of whether money is exchanged, would qualify as a "sale" of that personal information.

To the extent that a business is engaged in transfers that do qualify as a "sale," the business must provide a specialized notice of such activity, and provide consumers with the opportunity to opt-out of such sale. In particular, the business would need to (a) provide a clear and conspicuous link on its Internet home page titled, "Do Not Sell My Personal Information" that leads to a web page that enables a consumer, or a person authorized by a consumer, to opt-out of the sale of the consumer's personal information;[13] and (b) include a description of the consumer's rights to opt-out of the sale, including a link to the "Do Not Sell My Personal Information" web page within its online privacy policy, as well as any California-specific description of the consumers' privacy rights.[14] In addition, CCPA requires that businesses make available two or more methods for submitting consumer requests, including a toll-free number and a "Web site address" to opt-out.[15] Furthermore, if a business has factual knowledge that the consumer is less than 16, then the business must obtain affirmative authorization (i.e., prior opt-in consent) from consumer (between 13 and 16 years of age) and from consumer's parent or guardian (if less than 13) prior to engaging in a "sale" of such consumer's personal information.[16]

B. Disclosure Requirements

CCPA imposes specific requirements to notify consumers of the categories of personal information to be collected and the purposes for which those categories of information are to be used.[17] In addition, other elements of the CCPA impose certain disclosure requirements on businesses.

Categories of information and disclosures required for all privacy notices under the CCPA are as follows:

- Notice of the categories of personal information collected[18] in the preceding 12 months;[19]
- The categories of sources from which the personal information has been collected;[20]

---

[12] §1798.140(t)(1).
[13] §1798.135(a)(1).
[14] §1798.135(a)(2).
[15] §1798.130(a)(1). Note that the amended language proposed by Assembly Bill 1564, as modified by the Judiciary Committee, would, if passed, eliminate the requirement to provide a toll-free number for businesses that operate exclusively online.
[16] §1798.120(d).
[17] §1798.100(b).
[18] §1798.100(b) and §1798.110(c)(1).
[19] §1798.130(a)(5)(B). We note that §1798.130(c) specifies that the "categories of personal information required to be disclosed pursuant to [the notice provisions in CCPA] shall follow the definition of personal information in Section 1798.140." This raises the question of whether privacy notices need to be structured in a manner where each of the sub-points (A) through (K) in the definition of "personal information" should be treated as "categories" of personal information with individual discussions of the purposes of use of each such category. This interpretation would require a significant re-write of the vast majority of privacy policies. In practice, we expect most companies to assure that each of the sub-points in the definition of personal information are addressed (where collected), but not to substantially re-write the current descriptions of data collection, use, and disclosure.
[20] §1798.110(c)(2).

- Purposes of use,[21] and more specifically, the business or commercial purpose for collecting or selling personal information;[22]
- The categories of third parties with whom the business shares personal information;[23]
- The specific pieces of personal information the business has collected about the consumer;[24]
- Information about the consumer's rights of access and deletion;[25]
- A list of the categories of personal information about consumers that the business has disclosed for a business purpose over the prior twelve (12) months (or if it has not done so, it shall say that) by reference to the enumerated categories of data provided in the definition of "personal information" under the CCPA;[26] and
- If the business has not sold consumer personal information in the prior twelve (12) months, a statement providing that.[27]

In addition, to the extent that a business is engaged in the "sale" of consumer personal information, it must also provide the following categories of information and disclosures in its notices to consumers:

- Special notice that the personal information may be sold, and the right to opt-out;[28]
- Notice about sale and disclosure, and non-discrimination against those who opt-out;[29]
- If financial incentives are provided related to the business's use of consumer personal information, such as charging a different price or rate, or providing a different level or quality of goods or services to the consumer;[30]
- Two or more methods for submitting consumer requests, including a toll-free number and a "Web site address[;]"[31] and
- A list of the categories of personal information about consumers that the business has sold over the prior twelve (12) months by reference to the enumerated categories of data provided in the definition of "personal information" under the CCPA.[32]

---

[21] §1798.100(b).
[22] §1798.110(c)(3).
[23] §1798.110(c)(4).
[24] §1798.110(c)(5). Although this appears to be a requirement applicable to the content of a privacy notice generally, we appreciate it might not be feasible to comply in practice given that the specific pieces of data collected may vary from consumer to consumer (e.g., depending on what actual data fields a consumer completes in a web form). In addition, there is a tension between this requirement and §1798.130(a)(5), which appears to specify in greater detail what content needs to be provided in a privacy policy, and which does not require notice in the privacy policy of the specific pieces of personal information collected about that consumer, but rather specifies that notice must include relevant "categories" of personal information. In practice, we anticipate that a robust privacy policy combined with a tailored response to individual consumer access requests may be where most companies settle in terms of balancing these differing obligations.
[25] §1798.130(a)(5)(A).
[26] §1798.130(a)(5)(C)(ii).
[27] §1798.130(a)(5)(C)(i).
[28] §1798.135(a)(1)-(2).
[29] §1798.130(a)(5)(A).
[30] *Id*.
[31] §1798.130(a)(1).
[32] §1798.130(a)(5)(C)(i).

Baker McKenzie.

C. Data Subject Rights

i. Access

Similar to the GDPR, CCPA provides consumers with rights to access the personal information held about them by businesses in a readily usable format and one that, to the extent technically feasible, allows the consumer to transmit the personal information to another entity. Similar to the GDPR, the CCPA provides a time period for responding to such requests, forty-five (45) days in the case of the CCPA, which can be extended by an "additional 90 days" with notice to the consumer within the original forty-five (45) day response period that provides the reasons for the delay.[33] CCPA requires the following information be disclosed to consumers in response to an access request, which must cover the twelve (12) month period preceding the request[34]:

- Categories and ***specific pieces*** of personal information collected about that consumer;[35]
- The categories of sources from which the personal information is collected;[36]
- The business or commercial purpose for collecting or selling personal information;[37] and
- The categories of third parties with whom the business shares personal information.[38]

Similar to the GDPR, the CCPA provides that if the information provided in response to such a request from a consumer is provided electronically, it must be portable and readily useable to transmit to another entity;[39]

However, businesses are not required to respond to a consumer's access request more than twice in any twelve (12) month period[40] and businesses are allowed to charge a reasonable fee (or refuse to act on a request) if it is manifestly unfounded or excessive.[41] While an exhaustive list of what constitutes "manifestly unfounded or excessive" is not provided in the statute, the statute does provide that requests that are "repetitive" in character qualify under that standard.[42]

ii. Deletion

Similar to the GDPR, the CCPA provides data subjects with a right to deletion of certain personal information held by the business. CCPA requires that, upon verifiable consumer request, a business shall delete the consumer's personal information from its records and shall direct any service providers to delete the consumer's personal

---

[33] §1798.145(g)(1). Note that there is an ambiguity in the statute because another provision specifies that the original forty-five (45) day period can be extended for another forty-five (45) days (not ninety (90) days). §1798.130(a)(2). It is not clear how to read these provisions together. Ideally, there could be a stacking of all of these time periods so that a company would have 180 days to respond, but that is not clear.
[34] §1798.130(a)(2).
[35] §1798.110(a)(1) and (5).
[36] §1798.110(a)(2).
[37] §1798.110(a)(3).
[38] §1798.110(a)(4).
[39] §1798.100(d).
[40] *Id*.
[41] §1798.145(g)(3).
[42] *Id*.

Baker McKenzie.

information from their records.[43] The right to deletion, however, is not absolute, and the CCPA provides numerous exceptions to this right, many of which go beyond or are different than those provided under the GDPR. That is, a business shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or the service provider to maintain the personal information in order to:

- Complete the transaction, provide a good or service requested by the consumer or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer;
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity;
- Debug to identify and repair errors that impair existing intended functionality;
- Exercise free speech, ensure the right of another consumer to exercise free speech, or exercise another right provided for by law;
- Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 or Part 2 of the Penal Code;
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent;
- Enable solely internal uses that are reasonably aligned with the expectation of the consumer based on the consumer's relationship with the business;
- Comply with a legal obligation; or
- Otherwise use the personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.[44]

D. No Discrimination

CCPA contains an express non-discrimination requirement related to goods and services provided to consumers who opt-out of sale of their personal information by the business. It requires that businesses not discriminate against a consumer because a consumer exercised rights under CCPA, including but not limited to, by:

- Denying goods or services to the consumer;
- Charging different prices or rates, including through discounts or other benefits or imposing penalties;
- Providing a different level or quality of goods or services to the consumer; or
- Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.[45]

However, the CCPA does not prohibit businesses from charging consumers a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.[46] Furthermore, if a business is able to obtain the prior

[43] §1798.105(c).
[44] §1798.105(d)(1)-(9).
[45] §1798.125(a)(1)(A)-(D).
[46] §1798.125(a)(2).

opt-in consent of the consumer, it may offer financial incentives to the consumer to allow for the sale of her/his personal information, including:

- Payments to consumers as compensation for the collection of personal information, the sale of personal information, or the deletion of personal information; and
- Offering of a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data.[47]

III. ENFORCEMENT

The CCPA does not expressly allow for a private right of action for violations of the privacy provisions of the CCPA, and instead provides that "[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law[,]"[48] which seems intended to prohibit use of other statutes to support a private claim based on violation of the CCPA. The California Attorney General may also bring actions for injunctive relief and for civil penalties of $2,500 per violation, or up to $7,500 per violation if intentional, ***after*** notice and a 30 day opportunity to cure.[49] The amendments included in Senate Bill No. 1121 provide that enforcement by the Attorney General will be delayed until the earlier of six months from issuance of regulations or July 1, 2020.[50]

In addition, however, any consumer whose nonencrypted or nonredacted personal information that is part of a designated subset of personal information (i.e., (1) first name or initial and last name in association with: (i) social security number; (ii) driver's license number or state identification card number; (iii) account/credit card/debit card number and the necessary access code or PIN to access the account; (iv) medical information; (v) health insurance information; or (vi) information collected through the use or operation of an automated license plate recognition system; or (2) user name or email address in combination with a password or security question that would permit access to an online account) is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

- To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty dollars ($750) per consumer per incident or actual damages, whichever is greater;
- Injunctive or declaratory relief; and/or
- Any other relief the court deems proper.[51]

While the private right of action under the CCPA is, by the terms of the CCPA, limited to data security breach claims, it is expected that plaintiffs firms will seek to try other theories (e.g., unfair competition) to assert broader claims related to CCPA.

IV. APPLICATION TO NAA MEMBERS

[47] §1798.125(b). Note that there is an amendment proposed by Assembly Bill 846 that addresses the application of the anti-discrimination elements of the CCPA to customer loyalty programs.
[48] §1798.150(c).
[49] §1798.155(b).
[50] §1798.185(c).
[51] §1798.150(a)(1).

Baker McKenzie.

A. Addressing the "Sale" of Personal Information

A critical issue is whether or under what circumstances Members may engage in the "sale" of personal information about California residents to third parties. In this context, "sale" is defined broadly to include "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 by the business to another business or a third party for monetary or other valuable consideration."[52] In order to identify potential "sales" of personal information of California consumers, Members covered as businesses under the CCPA will likely need to conduct a certain amount of due diligence to determine: (i) what data categories are shared with outside recipients (e.g., vendors, affiliates, business partners); (ii) for what purpose is it shared; (iii) whether the recipient is restricted by contract from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services; and (iv) whether the individual "consumer" has directed the sharing of her/his data with the third party.

Some key elements to bear in mind during the diligence process and categorization of recipients that may provide for transfers or disclosures that fall outside of the scope of a "sale" under the CCPA:

- **Disclosures at the Direction of the Consumer:** The CCPA provides that a business does not sell personal information when a consumer "uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided that the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title."[53] This description may encompass where a consumer directs the Member to disclose personal information to a particular outside recipient or an affiliate. However, a key condition is that the Member should confirm that the third party recipient itself does not "sell" the data, or if it does, that such sale adheres to the notice and choice provisions in CCPA. There are several potential strategies to address these issues that may be discussed. One strategy, although untested, would be to update agreements with these recipients to specify that the Member is disclosing personal information to the recipient at the direction of the consumer to perform a transaction, and that the third party represents and warrants that they do not "sell" the data that the Member provides within the meaning of CCPA, or if they do, that they will provide appropriate notice, choice, and otherwise comply with CCPA.

- **Disclosures to Services Providers:** The CCPA provides that a business does not sell personal information if the recipient is a "service provider" that only uses the personal information to act on behalf of the business to carry out the specific "business purpose" (as defined by the CCPA)[54] for which the business provides the data (and does not use such data for any other purpose). This category may work well for IT support providers, certain security services, and others, provided that the service provider does not make any secondary use of the personal information for its own purposes (e.g., analytics). For disclosures to any such service providers, the Member must include the categories of such service providers in its privacy notice, and the service providers must be subject to appropriate contract terms and must cooperate with the business

[52] §1798.140(t)(1).
[53] §1798.140(t)(2)(A).
[54] "Business purpose" includes auditing, detecting security incidents, debugging, maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions.

Baker McKenzie.

if a consumer provides a verifiable request for access or deletion or the like. The service provider should also certify to the Member that it meets the data usage restrictions. We anticipate that the specificity of these requirements (e.g., the strict limits on use, the certification, and the like) could result in the negotiation of an amendment to certain of Members' existing service provider contracts (or at least the high priority arrangements), depending on the existing language of such contracts.

- **Disclosures to Other Businesses or Third Parties Where There is No Valuable Consideration for the Personal Information.** This may be a reasonably suitable fit for recipients that do not fall within the prior two categories (e.g., auditors or credit check companies, which act independently and not on behalf of the Member, and also which do not receive data as per any direction given by the individual). One strategy, again untested, would be to update agreements with such third parties to specify that they do not pay the Member any monetary or other consideration for the personal information, and they do not "sell" the data that the Member provides within the meaning of CCPA.

- **Disclosures to Affiliates.** Disclosures to affiliates may align with one of the categories above. For example, where a disclosure to an affiliate is done to perform a transaction on behalf of a customer, those disclosures could potentially be treated as done at the direction of the consumer. Where the disclosure is made to an affiliate as a service provider, it would likely fall outside of the scope of a "sale" under the CCPA, if the recipient Member is not permitted to use the personal information for its own purposes and meets the other requirements for "service providers" under the CCPA. Disclosures to affiliates outside of those two circumstances may need to be reviewed to determine whether they may qualify as a "sale" (e.g., affiliate's use the personal information to enhance their own consumer profiles or further customize or enhance their customers' experience), and, if so, how to address such disclosures in the context of CCPA. Further, we should note, that disclosures to affiliates may also need to be subject to a written agreement.

To the extent that a Member does engage in any "sale" of personal information, it must provide a specialized notice of such activity, and provide consumers with the opportunity to opt-out of such sale. In particular, the Member would need to (a) provide a clear and conspicuous link on its Internet home page titled, "Do Not Sell My Personal Information" that leads to a web page that enables a consumer, or a person authorized by a consumer, to opt-out of the sale of the consumer's personal information and (b) include a description of the consumer's rights to opt-out of the sale, including a link to the "Do Not Sell My Personal Information" web page within its online privacy policy, as well as any California-specific descriptions of consumers' privacy rights. [55] As noted above, the Member would need to provide two or more methods for submitting consumer requests, including a toll-free number and a "Web site address" to opt-out.[56] In addition, the Member would need to refrain from selling personal information for those consumers who have opted-out and ensure training for everyone responsible for handling consumer's requests.[57] It would also need to limit its use of personal information collected in connection with the opt-out request to only those purposes necessary to comply with the opt-out request.[58]

---

[55] §1798.135(a)(1)-(2).
[56] §1798.135(a)(1). Note that the amended language proposed by Assembly Bill 1564, as modified by the Judiciary Committee, would, if passed, eliminate the requirement to provide a toll-free number for businesses that operate exclusively online.
[57] §1798.135(a)(3)-(4).
[58] §1798.135(c).

Baker McKenzie.

Taken together, these requirements will necessitate a deep understanding of vendor, business partner, and affiliate transfers, determination of where such transfers or disclosures qualify as a sale, and, where they do, if and how such transfers or disclosures could be terminated upon receipt of an opt-out demand from a consumer. Furthermore, the CCPA's requirement that consumers not be requested to provide consent to the sale of their personal information for a period of at least twelve (12) months following such opt-outs may necessitate additional tracking and record keeping related to such opt-out requests.[59]

In practice, we anticipate that Members' arrangements with online behavioral advertisers, social media sites, and other third parties in connection with advertising and marketing may trigger these "sale" provisions. However, Members may be able to leverage current opt-out choice programs (e.g., via NAI and DAA programs), as well as cookie disclosures, to help address such requirements. We also expect the third parties within this ecosystem will be working to adapt their frameworks to CCPA requirements, and that the great majority of businesses will need to adopt more explicit CCPA disclosures (e.g., "Do Not Sell My Personal Information") such that adherence to these specifications should generally align with consumer experiences on other sites. [60]

B. Addressing Customer Rights Requests of Access and Deletion

To the extent that a business has implemented a GDPR data subjects rights response policy and procedure, it would likely be able to adapt that for application to the access and deletion rights under the CCPA without substantial changes. However, for those businesses that have not yet implemented such a policy or procedure, it will likely require additional diligence on the IT systems and processes necessary to comply with such a data subject rights request. Personal information of California consumers may be stored in multiple different databases and it may be difficult from a technical standpoint to automate the retrieval of that information for responding to access rights requests. In addition, it may be difficult to fully delete personal information from certain systems in a manner that maintains the integrity of the system or the processes that it provides. With that in mind, in conjunction with the due diligence efforts on identifying the categories and locations of personal information processed by Members, Members should also work with their IT departments and/or service providers to identify potential solutions (either automated or manual) to respond appropriately to access and deletion requests from California consumers within the statutory response period of forty-five (45) days.

C. Arbitration Clauses

While enforcement of the CCPA's privacy provisions is left to the California Attorney General under the statute, it may be the case that individuals in California attempt to use other California laws, including the California Unfair Competition Law, as a way to bring claims related to alleged violations of CCPA.[61] In a provision that appears targeted at arbitration clauses and class action waivers, the CCPA expressly invalidates waivers of rights to obtain

---

[59] §1798.100(d).

[60] The Digital Advertising Alliance has pushed the California legislature to allow the DAA's existing opt-out framework for cookies and related tracking technologies to apply to CCPA opt-out requests for "selling" such data.

[61] The CCPA expressly states that the private right of action provided for in this section applies only to data breaches, and further provides that nothing in the CCPA shall be interpreted as serving as the basis for a private right of action under any other law (§1798.150(c)). How this will apply in fact remains to be seen.

Baker McKenzie.

remedies under the CCPA.[62] However, the enforceability of this element of statute against businesses engaged in interstate commerce may be questioned in light of the Federal Arbitration Act, as the Federal Arbitration Act would likely preempt this language in the CCPA if sufficient consent to arbitration was obtained from the consumer. Application of the Federal Arbitration Act would likely require California courts to enforce arbitration of CCPA claims.[63] As such, Members may wish to analyze whether the use of arbitration provisions, to the extent not already included in agreements with California consumers, may be an element of their overall CCPA compliance and risk mitigation strategy.

V. CONCLUSION

The CCPA introduces new and challenging data privacy requirements for many businesses, including many Members of the NAA. While the specifics of the law are still subject to amendment, we expect that its fundamental requirements and the rights afforded by it to consumers will remain largely unchanged and we do not expect that a federal law preempting the CCPA to be made effective on or before the CCPA's operational date of January 1, 2020. Due to the differences between the CCPA and the GDPR, additional efforts, particularly around conducting diligence on data transfers and disclosures, will likely be required to be prepared for the application of the CCPA even for those Members that have a fulsome GDPR compliance program in place. For those Members that are subject to the CCPA that did not have to address GDPR compliance, the CCPA will introduce a completely new and novel set of compliance issues that will require significant diligence upfront, updating of notices, and implementation of back-end policies and processes. While there is still time to address these elements prior to January 1, 2020, Members are subject to the CCPA and have not yet begun the necessary action items for compliance should began to do so as soon as practicable.

[62] "Any provision of a contract or agreement of any kind that purposes to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable." §1798.192.

[63] *See*, e.g., *AT&T Mobility v. Concepcion*, 131 S. Ct. 1740 (2011), in which the Court ruled that the Federal Arbitration Act preempted California's prohibition of certain class action waivers because the prohibition was "an obstacle to the accomplishment and execution of the full purposes and objectives" of the Federal Arbitration Act.