Introduction

- In follow-up to our previous publications on the California Consumer Privacy Act (the "CCPA"), we have prepared in PowerPoint format the following overview of certain of the more significant provisions of the CCPA in order to assist our clients in navigating the challenging requirements that the CCPA imposes upon businesses.
- The CCPA has undergone numerous revisions since our office began following the issue in 2019.
- Earlier this year, the California Attorney General, the entity responsible for enforcing the CCPA, issued proposed Regulations in order to provide guidance to businesses on the proper implementation of the CCPA. We expect the Attorney General Regulations to be finalized in the coming weeks. Enforcement of the CCPA will begin July 1, 2020.
- You can access a more comprehensive publication on the updated CCPA and Regulations in our Alert, dated May 15, 2020, at the following link: https://www.brotherssmithlaw.com/publications/alert-the-california-consumer-privacy-act-updated-may-2020/.

The California Consumer Privacy Act ("CCPA")

What it is:

- A state law providing California residents with the rights to control the collection, use and sharing of their personal data.
- Part of a global trend toward stronger privacy protections and greater data transparency, as reflected in legislation such as the European Union's General Data Protection Regulation (the "GDPR") and the Canadian Anti-Spam Law.
- Took effect on January 1, 2020.
- Requires the Attorney General to adopt regulations in order to further the CCPA's purposes.
- The Attorney General issued draft Regulations, as modified, which provide guidance to businesses on how to comply.
- Enforcement by the Attorney General begins July 1, 2020.

Which businesses are covered by the CCPA?

- For profit businesses with annual gross revenues of at least $25 million;
- Businesses that buy, receive, sell or share the personal information of 50,000 or more Consumers, households or devices annually (i.e., 137 records per day). This category would cover a majority of businesses who have a website that captures the IP addresses of its visitors; and
- Businesses that derive at least 50% of their annual revenue from selling Consumers' personal information.

Bottom line: Virtually all but the smallest businesses without a website address are covered by the CCPA.

Important Definitions

- **Consumer:** A natural person who is a California resident, including employees.
- **Personal Information**: Any information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, *with a particular consumer or household*". This definition includes personal identifiers, commercial information, biometric information, internet activity such as the Consumer's browsing history, and inferences about the Consumer that may be drawn from any of the above information.
- **Sale**: The "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".

Consumer Rights

The rights of California Consumers under the CCPA can be categorized as follows:

1. Right to Know: The right to request that a business disclose the categories and items of Personal Information that the business has collected and shared about the Consumer (a "Right to Know").

2. Right to Delete: The right to request that a business delete the Consumer's Personal Information from the business' records (a "Right to Delete").

3. Opt-Out Right: The right to direct a business that "sells" Personal Information to third parties not to sell such information (an "Opt-Out Request").

Covered businesses are required to (i) post a notice to Consumers explaining the rights set forth above and (ii) respond to and comply with Consumer Requests to Know, Requests to Delete and Opt-Out Requests (collectively referred to as "Requests").

The Privacy Policy

- California Civil Code Section 1798.100: "A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used."
- The Privacy Policy is typically posted on the business' retail website and/or mobile application. The Privacy Policy should also be posted at the business' retail store location(s) and/or in business publications and written materials.
- California-Specific Notice: The Privacy Policy must include a California-specific description of the privacy rights of California Consumers. A business whose website already contains a privacy policy or notice that is compliant with previous California privacy laws or with the GDPR may be able to comply with the CCPA by adding the California-specific notice onto its existing privacy policy or notice.
- The California-specific notice must include the following information:
  - The categories of Personal Information that the business collects, the manner in which the Personal Information is collected from Consumers, how the Personal Information is used by the business and with whom the Personal Information is shared; and
  - The Consumer's rights under the CCPA, including the Right to Know, the Right to Delete and the Opt-Out Right, and the process by which the Consumer may exercise these rights;
  - A non-discrimination notice which states that the business shall not discriminate against the Consumer for exercising his/her rights under the CCPA;
  - Instructions on how an authorized agent can make a request under the CCPA on the Consumer's behalf;
  - Contact information for a representative of the business whom the Consumer may contact with questions or concerns about the business' privacy policies; and
  - The date on which the Privacy Policy was last updated.

Requests to Know and Requests to Delete

- Businesses are required to develop and maintain a system for responding to Consumer Requests to Know and Requests to Delete their Personal Information. The system should address the following:
  - Verify the identity of the requesting Consumer (if the Consumer maintains a password-protected account with the business, the business may verify the Consumer and respond to the Request through the Consumer's account);
  - Provide information that is responsive to a Consumer's Request to Know the categories and/or specific pieces of Personal Information that the business collected about the Consumer, and comply with a Consumer's Request to Delete;
  - Maintain procedures to track Requests, and avoid collecting Personal Information or requesting consent to collect Personal Information from a Consumer who requests deletion for 12 months after the Request;
  - Ensure that the business responds within 45 days after receipt of the Request, or informs the Consumer that the business needs an additional 45 days to respond; and
  - Maintain a record of Consumer Requests and how the business responded for at least 24 months.
  - Limitations:
    - The business may not charge a fee for responding to the Request, and may not require the Consumer to incur any indirect costs (e.g., by requiring a notarized affidavit or proof of identification).
    - The business is only required to provide Personal Information collected within the past twelve (12) months in response to a Request to Know.
    - Consumers can only make two (2) Requests per year.

Limitations on Responding to Requests to Know

- A business shall not disclose:
  - Social security numbers;
  - Driver's license numbers or other government ID numbers;
  - Financial account numbers;
  - Health insurance or medical ID numbers;
  - Account password or security questions and answers; or
  - "Unique biometric data generated from measurements or technical analysis of human characteristics".
- However: The business shall inform the Consumer "with sufficient particularity" that it has collected this type of information.
    - Example: The business shall notify the Consumer that it collects "unique biometric data including a finger print scan", without disclosing the actual fingerprint scan.
- A business is not required to "search" for a Consumer's Personal Information if the business meets all of the following requirements:
  - The business does not maintain the Personal Information in a searchable or reasonably accessible format;
  - The business maintains the Personal Information solely for legal or compliance purposes;
  - The business does not sell the Personal Information and does not use it for a commercial purpose; and
  - The business describes to the Consumer the categories of records that may contain Personal Information that the business did not search because the business meets the requirements above.

Opt-Out Rights

- A business is required to state in its Privacy Policy or Notice whether or not the business sells Personal Information, using the CCPA's broad definition of a "sale".
- A business that "Sells" the Personal Information of Consumers is required to:
  - Post a **clear and conspicuous** link on its website titled **"Do Not Sell My Personal Information"** or **"Do Not Sell My Info"**, which must …
    - Direct Consumers to an interactive web form by which the Consumer can submit the Opt-Out Request.
- The business has 15 business days to comply with the Opt-Out Request.
- The business is not required to verify the Opt-Out Request. However, the business may deny the Request if it has a good faith, reasonable belief that the Request is fraudulent.
- A business may not sell Personal Information of Consumers aged 13 to 15 unless the Consumer has affirmatively authorized the Sale (an "Opt-In"). A business may not sell the Personal Information of children under 13 years of age unless the Consumer's parent or guardian has affirmatively authorized the Sale.
  - A business that sells Personal Information shall implement procedures to determine the age of website visitors and to obtain the Opt-In consent of children aged 13 to 15 and the Opt-In consent of the parent or guardian of children under 13.
- A business that does not, and will not, "Sell" the Personal Information of Consumers is not required to provide an opt-out link. The business shall state in its Privacy Notice that it does not sell Personal Information.
- It remains to be seen how broadly the definition of a "sale" will be interpreted by the Attorney General and consumer advocates.
  - Note: Data analytics could be sufficient to constitute a sale. It is unclear at present exactly how broadly this will be interpreted by the Attorney General and/or the courts.

Non-Discrimination

- Under the CCPA, a business shall not discriminate against a Consumer because the Consumer exercised his or her rights under the CCPA, including, but not limited to, by:
  - Denying goods or services to the consumer;
  - Charging different prices or rates for goods or services, including through the use of 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.

Non-Discrimination and Rewards Programs

- What does non-discrimination mean for rewards programs and other financial incentive programs?
  - If a Consumer "opts-out" of the collection or sharing of his or her Personal Information and/or requests deletion, it may interfere with the Consumer's ability to participate in the rewards program.
  - However, a business may offer a financial incentive or price or service difference that is "reasonably related to the value of the Consumer's data".
  - Example #1: A clothing business offers a loyalty program where customers receive a $5-off coupon to their email address after spending $100 with the business. A Consumer submits a request to delete all personal information the business has collected about him/her, but also informs the business that he/she wants to continue to participate in the loyalty program. The business may deny the request to delete **only** as to the Consumer's **email address and the amount that the Consumer has spent with the business** because that information is necessary for the business to provide the loyalty program.
  - Example #2: A grocery store offers a loyalty program where Consumers receive coupons and special discounts when they provide their phone numbers. A Consumer submits a request to opt-out of the sale of his/her Personal Information. The grocery store complies with the request, but no longer allows the Consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store business can demonstrate that the value of the coupons and special discounts is reasonably related to the value of the Consumer's Personal Information to the business.

Data Vendors ("Service Providers")

- If the business shares Personal Information with vendors that process data for the business (known as "Service Providers" under the CCPA), this data sharing may be exempt from the requirements of the CCPA if both of the following requirements are met:
  - The business discloses in its Privacy Notice what types of Personal Information may be shared with Service Providers; and
  - The business has a written contract with the Service Provider that restricts the Service Provider from retaining, using or disclosing the Personal Information for any purpose other than for the specific purpose of performing the services specified in the contract.
- A Service Provider shall not sell data on behalf of a business if a Consumer has opted-out of the sale of their Personal Information with that business.

Penalties for Non-Compliance

- Attorney General Fines
  - The California Attorney General may fine businesses for failing to comply with the CCPA.
  - Fines may result from the failure to maintain compliant privacy notices and policies or to maintain appropriate opt-out procedures, failure to appropriately respond to Consumer Requests, discriminatory practices, non-conforming service provider agreements, etc.
    - It remains to be seen which aspects of the CCPA the Attorney General will prioritize when enforcement begins this summer.
  - The fines are as much as $2,500 per violation, and as much as $7,500 per intentional violation, with no limit.
  - The Attorney General may also obtain an injunction against a business for failing to comply.
- Lawsuits
  - Consumers have a private right of action, but only for data breaches.
    - The Consumer may sue even if the business was not at fault for the breach (such as in the event of a cyberattack) or the Consumer does not suffer harm as a result of the breach.
    - However, if the data is encrypted or redacted, the Consumer cannot make a claim.
  - Consumers may sue either individually or as a class.
  - The damages range from $100 to $750 per violation, or actual damages.
    - **Damages from a single data breach could add up to millions of dollars**.

How to Comply with the CCPA

Data Mapping: Prepare data maps, inventories or other records of all Personal Information collected by the business that pertains to California residents, households and devices, as well as information sources, storage locations, usage and recipients;

Privacy Policy: Update the privacy policy or notice on the business' website in order to cover the newly required information, including a description of California residents' rights under the CCPA and how to exercise Requests to Know, Requests to Delete and Opt-Out Requests;

Receiving Requests: Make available designated methods for Consumers to submit Requests pursuant to the CCPA, including, at a minimum, a toll-free telephone number if the business has retail locations. If the business "sells" Personal Information, provide a "Do Not Sell My Personal Information" button that links to an interactive webform which allows Consumers to submit an Opt-Out Request;

Data Security Systems: Implement appropriate data security measures in order to protect Personal Information, and maintain an incident response plan in the event of a data breach;

Employee Training: Train employees on how to handle Consumer inquiries and Requests and how to direct Consumers to exercise their rights under the CCPA; and

Service Provider Agreements: Review and update vendor service agreements. Formulate policies and procedures for vendors and other third parties who have access to Personal Information.

Current Events: How will COVID-19 affect the CCPA?

- Enforcement: The Attorney General will not delay enforcement of the CCPA due to business impacts related to COVID-19, despite requests from dozens of businesses, trade associations and industries.
- Network Security: Businesses should prioritize their data security networks in order to defend against data breaches. As a result of the Shelter-In-Place orders, many employees are working from home, potentially on unsecure devices or networks. Hackers may view the increase in virtual work and commerce as an opportunity.
- Operational Impacts: Businesses that screen the temperature of employees and/or customers prior to entering the premises could be considered to collect Personal Information. Businesses should avoid collecting any Personal Information (such as name, address, email or telephone number) other than the temperature reading, in order to ensure that the temperature information is not capable of being associated with a particular individual. The business should also avoid retaining records of temperature readings. If the business maintains a record of its employees' temperature readings, the business is required to comply with any requirements of the CCPA that may apply to that Personal Information, including providing a CCPA-compliant notice at the point of collection.

How Brothers Smith LLP can assist:

- Review and preparation of privacy policy
- Review, preparation and revision of service provider agreements
- Compliance advice
  - Responding to Consumer requests
  - Employee notices and training
  - Data privacy implications in transactions and litigation
- Tracking legislative developments, Attorney General advisories, and enforcement trends
- Vendor referrals