CCPA - For CA Businesses & Beyond

December 4, 2019

Presented by

Susan Kohn Ross

Co-presented by

SCGLEGAL

A WORLDWIDE NETWORK OF LEADING LAW FIRMS

Background

- The CCPA takes effect on January 1, 2020.
- The related regulations are now proposed (subject to comment) and will be finalized in time for their July 1, 2020 effective date.
- The CCPA requires companies to institute new internal data privacy regimes.

Threshold Questions

- What data is collected?
- From whom/what sources?
- What do you do with the data?
- Where is it stored?
- How long do you keep it?
- What about any marketing databases?
- What about processing payments?
- Who has access to it?
  - "Need to know" best practice
  - User name and password combinations unique to each user
  - Change the default password on all hardware and software when installed

What Is Involved?

- What are the processes and procedures the business will implement to address these consumer rights:
  - Notice
  - Access
  - To Be Forgotten
  - Opt-Out re Sale of Info
  - Receive services on equal terms

How do we store the data?

- Do we encrypt it?
- Do we aggregate?
- Do we deidentify it?
- Do we redact it?

Consumer Rights

- California consumers now have the right to know in advance the categories and details of any personal information collected and the related purposes and uses, along with the sources from which the data was collected and the third parties with whom the business shares or sells the personal information;
  - ∞ Additional purposes/uses cannot be implemented without consumer pre-approval.

When?

- The consumer must be informed "to, at or before" the point of collection about the categories of personal information to be collected and the purposes for which that data will be collected/used.

Covered Parties

1) Annual gross revenues in excess of $25 million (not limited to California revenue alone);

2) Companies which alone or in conjunction with others annually buy, sell, receive or share for commercial purposes, the personal information of 50,000 or more consumers, households, or devices;

or

3) Companies which derive 50% or more of their annual revenues from selling consumer personal information.

Non-Profits and Government entities are not subject to the CCPA

Exemptions

- California Confidentiality of Medical Information Act
- Health Insurance Portability and Accountability Act
- Health Information Technology for Economic and Clinical Health Act
- Federal Policy for the Protection of Human Subjects - clinical trial
- Personal information collected, processed, sold, or disclosed pursuant to a specified federal law relating to banks, brokerages, insurance companies, and credit reporting agencies, among others - Gramm-Leach-Bliley Act
- California Financial Information Privacy Act.
- Driver's Privacy Protection Act of 1994,
- If infringe on the noncommercial activities of newspapers and periodicals.

Internal Data Uses

- If the data collection is for the purposes of a job applicant, an employee, owner, director, officer, medical staff member of contractor of the business, such actions are exempt for one year - until January 1, 2021.
- Emergency contact and data needed to administer benefits is similarly exempted.

Required Disclosures

- The privacy policy must include a description of the consumer's rights under the CCPA, how he or she may submit requests for disclosure, deletion and opting-out, and, of course, additional information about data collection and sharing practices.
- Notice may be provided through a link to the relevant section of the online privacy policy.

Personal Information

- " … 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. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:"
- (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

- (B) Any categories of personal information described in subdivision (e) of Section 1798.80.
- (C) Characteristics of protected classifications under California or federal law.
- (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- (E) Biometric information - not further defined.

- (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
- (G) Geolocation data.
- (H) Audio, electronic, visual, thermal, olfactory, or similar information.
- (I) Professional or employment-related information.

- (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act.
- (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Civil Code § 1798.80

- Plus: signature, physical characteristics or description, telephone number, state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

Personal Information Excluded

- "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information.
- "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.
- Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.

Also Exempt

- Single, one-time transactions are exempt provided no sale of the information occurs to any third party, or if not maintained as personal identification.

Data Breach Notice - AB 1130

Expanded definition of personal information, which now includes any of the following: first name or initial and last name in combination with "any one or more of the following data elements, when either the name or the data elements are not encrypted:

- (A) Social security number.
- (B) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

Data Breach Definitions

- (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- (D) Medical information.
- (E) Health insurance information.
- (F) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

Remaining Definitions

- (G) Information or data collected through the use or operation of an automated license plate recognition system, [as defined elsewhere in the law]
- (2) A username or email address, in combination with a password or security question and answer that would permit access to an online account."

Consumer

- " ... [A] natural person who is a California resident … , however identified, including by any unique identifier."

Household

- "… [A] person or group of people occupying a single dwelling."

Device

- "… [A]ny physical object that is capable of connecting to the internet, directly or indirectly, or to another device."

Business Purpose Defined

- "… [As] the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected.

Business Purposes Are:

- (1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
- (2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
- (3) Debugging to identify and repair errors that impair existing intended functionality.

- (4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
- (5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

- (6) Undertaking internal research for technological development and demonstration.
- (7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

Privacy Policy

- Means a statement the business provides describing its practices on and off line regarding the "collection, use, disclosure and sale of personal information and of the rights of consumers regarding their own personal information."
- Must be posted online with a conspicuous link using the word "Privacy" on the home or landing page.

Sale

- "Sell," "selling," "sale," or "sold," means 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.

Not a Sale

- Data is shared at the direction of the consumer, even with third parties.
- Uses the data to accomplish the consumer's opt-out instruction.
- Shares the data with a service provider to perform a business purpose.
  - Must give notice to the consumer and the service provider does not sell or use the data for any other purpose.
- M&A, bankruptcy or other transaction where third party takes control of all or part of the business and there is no change in the data uses.

Right to Review

- California consumers have the right to demand the specific information being maintained about them, no more than twice in a 12 month period, subject to verification of the identity of the requesting party.
  - The 45 day period starts upon receipt of the consumer request.
  - Initial acknowledgment is due at 10 days - explain what the company will do and when to expect the completed response.
  - Explain appeal rights if deny request, even in part.
  - May charge for excessive requests.

Additional Rights

- Businesses are given 45 days to respond, although if "reasonably necessary" and the consumer is given notice, a total of 90 days to respond is possible.
- The information disclosed to consumers must be delivered free of charge and in as useable a portable fashion as possible.
- How will you handle incomplete requests?
- How will you notice appeal rights?

Verification

- Consider the sensitivity of the information and the risk of harm from unauthorized access or deletion.
- The process must be reasonable and seek only minimal additional data as warranted.
- Use an existing password protected account.
- Non-account holders - 2 or more data points - in some cases a declaration under penalty of perjury.
- High degree of certainty as to the requestor's identity.

Verification - Cont.

- What is the likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent should be the verification process.
- 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.

Opt Out

- California consumers will also have the right to opt out of having their personal information sold or disclosed and companies are mandated to conspicuously provide instructions for doing so by way of a link entitled ***"Do Not Sell My Personal Information***" or ***"Do Not Sell My Info"***
  - Prominently placed either on the home or landing page or that page which is directed to California consumers.
  - Attorney General will develop recommended logo - after public input.
  - Applies if any personal data is sold or shared.

Opt-Out - No?

- If the business does not sell or share/disclose personal data, it is exempt from the opt-out requirement.
- Cannot discriminate as to who may opt out, which includes denying goods or services, charging different prices or rates, or providing a different level of service or quality of goods.
- Unless those differences are reasonably related to the value provided to the business by the consumer's data.
- Loyalty and financial incentive programs are still allowed but are subject to specific notice requirements and must involve good faith estimates as to cost/value.

Right To Be Forgotten

- California consumers will also have the right to be forgotten, unless the data is necessary for the business or service provider for legitimate uses, such as completing the transaction and security and system integrity reasons.
- GDPR contains the right of the consumer to correct information, there is nothing comparable in this law.

Data of Minors

- Data of those 16 and younger cannot be sold absent affirmative opt-in consent by minors between 13 and 16, and by a parent or guardian for those under 13.

Enforcement - Originally

- In the hands of the Attorney General with fines capped at $7,500 per violation.
- Class action and private right of action are specifically barred.
- Consumer may file a civil action if his or her "non-encrypted or non-redacted" personal information is the subject of a breach.
  - Damages limited to between $100 and $750 per consumer per incident or actual damages, whichever is greater.
- Consumer does have the right to seek injunctive or declaratory relief or any other relief the court deems proper.

Enforcement Changed

- Now, any consumer whose "non-encrypted and non-redacted" personal information is subject to "unauthorized access and exfiltration, theft or disclosure" as the result of the businesses failure to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" may sue.
- The plaintiff is, however, limited to recover no less than $100 and no more than $750 per consumer per incident or actual damages, whichever is greater, along with injunctive or declaratory relief and any other relief the court deems proper.
- In reaching its decision, the court is instructed to "consider any one or more of the relevant circumstances …, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, and the defendant's assets, liabilities and net worth."

Claims

- Prior to initiating any civil action, the consumer must provide the business with 30 days' written notice identifying the violations alleged by reference to the specific provisions of the CCPA.
- If the business is able to cure, does so within that 30 day period and provides express written notice about the cure and assurances that no further violations will occur, neither an individual nor class action lawsuit may be brought.
- No notice is required to recover "pecuniary" damages, i.e., out of pocket costs.
- If violations continue, the consumer may sue to enforce the written statement and pursue statutory damages for violation of the written assurance and other rounds. However, any such lawsuit may rely only on violations of the CCPA and no other grounds for recovery.

Don't Forget

Not required under CCPA but good business practice dictates including -

- Data security
  - Written policies and procedures
  - Incident response plans
  - Appropriate / "reasonable"
- Service provider contracts
  - Vendor management / indemnity

Questions?

Thank You

Susan Kohn Ross, Esq.

Mitchell Silberberg & Knupp LLP
2049 Century Park East
18th Floor
Los Angeles, CA 90067
T: (310) 312-3206
F: (310) 231-8406
skr@msk.com | www.msk.com