

California Consumer Privacy Act

Robert K. Olsen, Esq.
Aldrich & Bonnefin, PLC
Nicholas C. Adams, Esq.
Bank of the West

CCPA

- ▶ New CCPA becomes effective on Jan 1, 2020
- ▶ Covered Persons
 - ▶ CCPA applies to “business” that collects, shares, discloses, processes or sells “consumer’s” personal information

CCPA

▶ “Business”

- ▶ Any legal entity organized or operated for profit or financial benefit of shareholders or owners, does business in CA and
 - ▶ Annual gross revenues \$25 million+
 - ▶ Buys, receives for business’ commercial purposes, sells, or shares for commercial purposes personal information of 50,000+ consumers
 - ▶ Derives 50% or more of annual revenues from selling consumer’s personal information

CCPA

- ▶ **Common control businesses**
 - ▶ Any entity that controls or is controlled by a business and that shares common branding
 - ▶ Treated as one “business”
 - ▶ Your BHC?
- ▶ **“Consumer”**
 - ▶ Natural person who is a CA resident

Covered Information

- ▶ CCPA applies to consumer's personal information
 - ▶ “Personal information” identifies, relates to, describes, is *capable of being associated* with particular consumer or household
 - ▶ *Not limited* to personal, family or household purposes

Covered Information

▶ Categories of personal information include:

- Name, address
- Protected classifications under CA or federal law
- Commercial information
- Biometric information
- Health insurance information
- Internet or other electronic network
- Geolocation data
- Audio, electronic, visual thermal, olfactory, or similar
- Professional or employment-related information
- Education information
- Inferences

Exempt Information

- ▶ Exclusions from “personal information”
 - ▶ Aggregate consumer information
 - ▶ Publicly available (governmental) information
 - ▶ Deidentified information
- ▶ Exceptions require robust technical barriers to re-identification

GLBA-CFIPA Exemption

- ▶ Personal information covered by GLBA or CFIPA is exempt from CCPA
- ▶ GLBA and CFIPA only apply to
 - ▶ “True” consumers (personal, family or household purpose)
 - ▶ Info collected for financial product or service
 - ▶ Includes applicants but not prospects

Net Result under CCPA

- ▶ Business purpose information is covered as to individuals
 - ▶ Sole proprietors*
 - ▶ Individual signers, guarantors, etc. on business or commercial accts, loans*
 - ▶ Prospects - business or personal
 - ▶ Employees, contractors, job applicants*
 - ▶ Vendor and other third party relationships*
- ▶ Other information you collect
 - ▶ Information not obtained in connection with providing financial product or service
 - ▶ (Information you buy)

*May be subject to change via amendment

Pending Amendments to the CCPA

- ▶ **Business to Business (B2B) Exemption:** If Governor signs, Assembly Bill (AB) 25 would add a new B2B exemption in Section 1798.145(m) [or (n)]
 - ▶ PI reflecting written or verbal communication or a transaction between covered business and consumer exempt from Sections 1798.100 (Right to Access), .105 [Right to Delete], .110 [Right to Know], .115 [Right to Know], 1798.130, and 1798.135 if:
 - ▶ Involved Individual: The consumer is a natural person acting as employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit, or government agency [“Entity”]; and
 - ▶ Business Context: The communications or transaction with the business occur solely in context of the business conducting due diligence regarding, or providing or receiving a product or service to or from, the Entity
 - ▶ Sunset: Provision sunsets on January 1, 2021

Pending Amendments to the CCPA

▶ Employment Exemption: New section 1798.145(g) [or (h)] excludes:

“Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person’s [PI] is collected and used by the business solely within the context of the natural person’s role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.”

- ▶ Employment exemption does not apply to sections 1798.150 (civil liability) or 1798.100(b) (initial disclosure). Thus, covered businesses still must provide employees with an initial disclosure and remain subject to CCPA’s civil liability provisions (hopefully only as to employment-related PI)
- ▶ But seems broad enough to exclude all employment related PI as well as independent contractors
- ▶ Sunsets on January 1, 2021

Pending Amendments to the CCPA

- ▶ Clarifying Revisions. AB 1355 and AB 25 would make a number of technical revisions to the CCPA which help clarify some of the existing ambiguities, including:
 - ▶ Revise references in Section 1798.110(c) from “that consumer” to “consumers” to reflect that this is a general disclosure obligation.
 - ▶ Revise Section 1798.110(c)(5) to clarify a business must disclose, “That a consumer has a right to request the specific pieces of [PI] the business has collected about that consumer” in the Online Privacy Policy.
 - ▶ Revise Section 1798.130(a)(5)(A) to require a business to provide a description of the consumer’s rights under Section 1798.100 (Right to Access) and Section 1798.105 (Right to Delete) in the Online Privacy Policy.
 - ▶ Revise Section 1798.130(a)(2) to clarify that a business “may require authentication of the consumer that is reasonable in light of the nature of the personal information requested”

CCPA-Right to Access

- ▶ Initial disclosure
 - ▶ Categories of PI collected and its purposes
 - ▶ Inform consumers of categories of personal information disclosed for a business purpose
- ▶ No further collection or use without disclosure
 - ▶ Disclosure limits future uses of PI

CCPA-Right to Access

- ▶ Triggered by collecting information (not limited to customers)
- ▶ Access to personal information
 - ▶ Disclose categories and specific pieces of info
 - ▶ 45-90 days after receiving verifiable consumer request
 - ▶ Maximum 2 requests per 12-month period
 - ▶ CCPA does not define “specific pieces of personal information”
 - ▶ Stay tuned for attorney general’s regulations

Right to Delete

- ▶ Delete collected information
 - ▶ Upon receipt of “verifiable consumer request”
 - ▶ “which the business has collected from the consumer”
- ▶ No deadline in statute, 90-day implied
- ▶ See complete list of exceptions on p. 25-26
 - ▶ Ongoing relationship; protect against fraud, legal obligation, internal “expectations” catch-alls
- ▶ Make sure vendor contracts give you the right to delete personal information when required by CCPA, or to have your vendor cooperate with you in responding to requests and making deletion determinations

Right to Know

- ▶ Consumer has right to request what information a business “collects,” “sells” and “discloses for a business purpose,” the sources of that information, and the non-vendor third parties with whom it is shared

Right to Know

- ▶ Collected information
 - ▶ Upon receipt of verifiable request, business must provide
 - ▶ Categories of personal information collected
 - ▶ Categories of sources
 - ▶ Purposes for collecting or selling
 - ▶ Categories of third parties (but not “service providers”) with whom business shares personal information
 - ▶ *Specific pieces* of personal information
 - ▶ Overlaps with right to access but not identical

Selling Information

- ▶ If PI is sold, disclose on request
 - ▶ Categories of PI collected
 - ▶ Categories sold
 - ▶ Categories of third parties info sold to
- ▶ “Sell” defined broadly
 - ▶ Sharing with service providers is not “sale”
 - ▶ Sharing pursuant to a consumer’s explicit direction not “sale”
 - ▶ Transfer of PI as part of a merger or acquisition is not “sale”
 - ▶ Be sure vendor contracts fit within “service provider” definition
 - ▶ Limit use of PI to specific contracted services
 - ▶ Add “CCPA addendum” to all vendor k’s?

Disclose for a Business Purpose

- ▶ Business must disclose what PI it shared for business purpose (non-sales)
- ▶ Must disclose upon verifiable written request
 - ▶ Personal information collected
 - ▶ Personal information disclosed

Right to Opt Out

- ▶ Opt out
 - ▶ Consumer has the right to direct a business that sells personal information not to sell consumer's personal information
 - ▶ “Do Not Sell My Personal Information” link

What is a sale?

- ▶ CCPA definition may be broad enough to cover almost any commercial transfer, even if no \$\$ exchanged
 - ▶ Service provider exception
 - ▶ Business shares with service provider
 - ▶ Perform business “operational” purpose
 - ▶ Notice provided to each individual of general opt-out rights
 - ▶ Vendor Management
 - ▶ Scrutinize referral agreements
- ▶ Business prohibited from selling information of consumers under 16 years of age

Right to Equal Service

- ▶ Anti-discrimination

- ▶ Business may not discriminate by

- ▶ Denying goods or services

- ▶ Charging different prices or rates

- ▶ Providing different level of quality

- ▶ *Suggesting* consumer will receive different price or rate

- ▶ Financial incentives

- ▶ Business is allowed to offer certain incentives if requirements are met

Response Procedures

- ▶ Verifiable consumer request
 - ▶ Stay tuned for regs
- ▶ 45 deadline (extendable to 90), but must notify of extension
- ▶ Identify consumer with information provided in verifiable request
- ▶ 12 months of activity
- ▶ Limit of 2 access requests per year - can charge fee or refuse if “manifestly unfounded or excessive”
- ▶ Enumerated categories of personal information
- ▶ Information must be provided in writing and delivered “through consumer’s account”

Online Privacy Policies

- ▶ The following must appear wherever online privacy policies are located
 - ▶ General description of consumer's rights
 - ▶ Categories collected
 - ▶ Categories sold in preceding 12 months
 - ▶ Categories disclosed

Practical Considerations

- ▶ Implementation Tips and Reminders
 - ▶ Start as early as possible
 - ▶ Engage broadly - business lines, records and information managers, compliance, risk, legal
 - ▶ Know what you DON'T need to search
 - ▶ Dating information helps - 12 month access lookback
 - ▶ Some material may need to be disclosed but not deleted (i.e. legal hold) or may not be able to be disclosed at all (i.e. SARs)
 - ▶ “Publicly available” is defined narrowly
 - ▶ “Business” is defined expansively
 - ▶ Vet public disclosures in advance of Jan. 1
 - ▶ Deletion exemptions are useful for financial institutions
 - ▶ Leverage existing GDPR, CAN-SPAM, customer call center, subpoena response, and record retention programs

Practical Considerations

- ▶ Access and Deletion Request Intake
 - ▶ Need both online and phone channels*
 - ▶ Authentication method must work for customers and non-customers*
 - ▶ Expect fraudsters and spammers
 - ▶ Automation - tradeoff of design and implementation costs vs. improved response time if high volumes, consistency
 - ▶ Business/Risk decision - screening out non-CA, GLBA and other exempt requestors
 - ▶ Keep it scalable - new state and/or federal laws will likely add requirements, exemptions may sunset

*May be subject to change via amendment, AG regs

Practical Considerations

▶ Personal Information Search

- ▶ Importance of having data inventories - know where to search for different types of requestors
- ▶ Search must be able to identify the type of requestor (i.e. GLBA, commercial customer, prospect, etc.)
- ▶ Some data types are harder to search than others (audio recordings, backups, unstructured data, e-mails, photos)
 - ▶ May be hosted locally, on cloud, or off-premise
- ▶ Some manual review likely necessary to weed out false hits
- ▶ Consolidating duplicates - may have a requestor's PI located on five different systems or databases, only need to disclose once
- ▶ Disclosure search may be limited to past 12 months, deletion search must go back farther

Practical Considerations

▶ Responding to Requests

- ▶ Multiple delivery methods for responding - via existing account, “by mail or electronically at the consumer’s option”*
- ▶ Must be secure, but can’t force consumer to create an account to receive response*
- ▶ May want to use templates and standardized language, but access requests require a personalized response
- ▶ Keeping customers happy - giving exempt customers substantive but standardized information
- ▶ Avoid unintentional repopulation via suppression lists
- ▶ Leverage statute’s existing “categories”

*May be subject to change via amendment, AG regs

Practical Considerations

- ▶ **Managing Third Parties and Service Providers**
 - ▶ Service provider definition very technical, requires contract review
 - ▶ Third parties do not receive deletion notices, but must be disclosed
 - ▶ Carefully review sales and referral arrangements to avoid accidental “sale”
 - ▶ Affirmative consent or service provider safe harbors
 - ▶ Build CCPA compliance into overall vendor management process - procurement, due diligence, contracting, and onboarding

Practical Considerations

▶ Do-Not-Sell

- ▶ Use existing opt-out tracking systems
- ▶ If you don't sell, say so!
- ▶ “Homepage” defined broadly - includes “any Internet Web page where personal information is collected” and app download or settings page

▶ Employee Training

- ▶ Funnel CCPA requests
- ▶ Know what is in and out of scope
- ▶ No search or deletion surprises

Liability Under CCPA

- ▶ Private right of action and attorney general enforcement
 - ▶ Statutory damages
 - ▶ Liability for data breach (even though CCPA sets no info sec standards)
 - ▶ PI definition is more limited for data breaches
 - ▶ Breach of express written statement
 - ▶ Consumer may initiate action against business to enforce written statement

Thank You

- ▶ Nicholas C. Adams
- ▶ Bank of the West
- ▶ Nick.Adams@bankofthewest.com

- ▶ Robert K. Olsen
- ▶ Aldrich & Bonnefin, PLC
- ▶ Rolsen@ABlawyers.com