Privacy Is Coming An In-Depth Analysis of the California Consumer Privacy Act (CCPA)

April 30, 2019

California Consumer Privacy Act (CCPA)
A Brief History

- **Originally introduced in the California Legislature in 2017**
- **Ballot initiative filed after CCPA bill deemed inactive**
  - Early summer 2018, over 600,000 signatures collected
  - Would have appeared on ballot in November 2018
  - CCPA (AB-375) was resurrected on June 21, 2018 and became law on June 28, 2018
  - Passage of CCPA was contingent on withdrawal of ballot initiative
- **Subsequent developments**
  - CCPA was amended once (SB-1121) on Sept. 23, 2018
  - CCPA becomes effective on January 1, 2020
  - Several competing amendments have been proposed

Bradley

California Consumer Privacy Act

- High Level Overview
  - Eight “Consumer” or Individual Rights
    - General Disclosures
    - General Notice and Website Privacy Policy
    - Verifiable Request
    - Opt-out requirement for information sold
    - Opt-in requirement for children (under 16)
    - Access and Portability
    - Deletion
    - Equal services on equal terms
  - Additional Business Obligations
    - Train employees
    - Execute vendor and service provider contracts with specific criteria
    - Create methods for consumer to exercise rights
  - Security required
  - Private right of action for data breach

Bradley

CCPA vs. Existing U.S. Privacy Law

Business Requirements	U.S. Federal Laws	Most U.S. State Laws	CCPA
Applies to a broad range of companies and not limited to distinct industries (e.g. health care or finance)	✗	✗	✓
Applies to the collection of personal information online and offline	Depends	✗	✓
Provide detail information on how they use and process the personal information collected	Depends	✗	✓
Notify individuals about the right to access information held about them	Depends	✗	✓
Notify individuals about a right to have their information deleted	Depends	✗	✓
Include a “Do Not Sell” my personal information link on websites and privacy notices	✗	✗	✓
Describe the information that they share with service providers	✗	✗	✓
Describe the types of entities to whom they sell information	✗	✗	✓

Bradley

California Consumer Privacy Act (CCPA)

- Applicability – does business in CA and -

Buys, sells, or shares personal information of 50,000 'consumers' or devices

Gross revenue is greater than $25 Million

Derives 50% of annual revenue from sharing personal information

Bradley

What is a Business under CCPA?

- Sole proprietorship
- Partnership
- LLC
- Corporation
- Association
- Other legal entity not considered a non-profit
  - Non-profit is defined under California Nonprofit Corporation Law

NOTE: Be aware of business that controls a non-profit and that shares common branding (shared name, servicemark, or trademark) with a non-profit

Bradley

What does it mean to "do business" in California?

- CCPA does not define "doing business"
- California Revenue and Taxation Code = "actively engages in any transaction for the purpose of financial or pecuniary gain or profit in California"
- Also includes:
  - Physical presence (may include where servers are located)
  - Employees in CA
  - Holding a license to conduct business in CA
  - Real or personal property of the business in CA that exceeds $50K
  - CA sales exceed $500K or 25% of business's total sales
- Be aware of "common branding" with CCPA covered entity

Bradley

Expanded PII Definition

(1) “Personal information” means . . . is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

(A) Identifiers such as . . . Internet Protocol address, email address. . .

(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.

. . .

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer . . . .

General Disclosures

- At or before collection, business must disclose description of:
  - Categories of PI to be collected and the purposes for which the PI shall be used
  - Consumer's right to request deletion
  - Consumer's right to request disclosure regarding collection of PI
  - Consumer's right to request disclosure regarding sale of PI
  - Consumer's right not to face discrimination for exercising right under CCPA

General Disclosures

- Lists of categories for preceding 12 months:
  - Categories of PI collected about consumers, including
    - Categories of PI collected about that consumer*
    - Categories of sources from which the PI is collected
    - Business or commercial purpose for collecting or selling
    - Categories of third parties with whom the business shares PI
    - Specific pieces of PI business has collected*
  - Categories of PI sold about consumers
  - Categories of PI disclosed about consumers for a business purpose

Bradley

Disclosures for Financial Incentives

- Business must disclose:
  - Notice of any financial incentives for the collection, sale, or deletion of personal
  - Clear description of material terms of any financial incentive program

Bradley

Website Disclosures (Privacy Policy)

- Method for consumer to submit a request for disclosure of collection of PI and disclosure for sale or disclosure for a business purpose of PI
- Include in online privacy policy and any CA specific disclosure (or website if neither of those maintained)
  - Consumer's right to request disclosure regarding collection of PI
  - Consumer's right to request disclosure regarding sale of PI
  - Consumer's right not to face discrimination for exercising right under CCPA
  - Lists of categories for preceding 12 months:
    - Categories of PI collected about consumers
    - Categories of PI sold about consumers (or none)
    - Categories of PI disclosed about consumers for a business purpose (or none)

Bradley

Website Disclosures (Privacy Policy)

- Include in online privacy policy and any CA specific disclosure
  - Description of consumer's right to opt out of the sale of PI
  - Link to Do Not Sell My Personal Information webpage
  - Description of the consumer's right to request deletion
- Must update "preceding 12 months" disclosures at least once every 12 months
- Must also provide "clear and conspicuous link" titled "Do Not Sell My Personal Information" that enables a consumer to opt out of the sale of personal information.

Bradley

Verifiable Consumer Requests

- Requests for information collected, sold, or shared for a business purpose
- Two or more reasonably accessible methods
  - Toll free number and second method (web page)
- Step 1: Identify the type of request (if other than deletion)
- Step 2: Verify the consumer (or registered agent authorized by consumer)
  - Business does not have to comply if it cannot verify
  - AG will adopt regulations for verification
- Must respond within 45 days
- Must deliver free of charge (unless manifestly unfounded or excessive -> reasonable fee)

Bradley

Consumer Requests - Response

- To respond to a consumer's request for disclosure regarding the collection of personal information:
  - Categories of PI collected about that consumer in preceding 12 months
  - Categories of PI collected about that consumer
  - Categories of sources from which the PI is collected
  - Business or commercial purpose for collecting or selling
  - Categories of third parties with whom the business shares PI
  - Specific pieces of PI business has collected about the consumer

Bradley

Consumer Requests - Response

- To respond to a consumer's request for disclosure regarding the sale of personal information:
  - Categories of PI sold about that consumer in preceding 12 months
  - Categories of PI the business has sold about consumers in preceding 12 months

Bradley

Consumer Requests - Response

- To respond to a consumer's request for disclosure regarding the disclosure for a business purpose of personal information:
  - Categories of PI disclosed about that consumer for a business purpose in preceding 12 months
  - List of third categories of third parties to which the consumer's personal information was disclosed for a business purpose in the preceding 12 months
  - Disclose a list of categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months.

Right to Opt-Out of sale

- As noted, specific link must be provided, included in privacy policy
- Third parties have to be prohibited from re-selling unless consumer was provided explicit notice and opportunity to opt-out of that sale
- If opt-out
  - Must refrain from selling consumer's PI collected by business without express authorization
  - Cannot request authorization for at least 12 months

Bradley

Opt-in Requirement For Children

- A business shall not sell the personal information of anyone under 16; unless
  - Business receives an affirmative opt-in
    - Under 16 must affirmatively opt-in to sale or parent/guardian
    - Under 13 with parent or guardian affirmative authorization only
  - Imperative to document affirmative consent for any individual under 16 and update policies and procedures to reflect process for confirming age
  - Incorporate into employee training

Access and Portability

- "Disclose and deliver" required information to consumer free of charge within 45 days of receiving request
- Disclosure of personal information collected, sold, or shared (for business purpose) can be provided:
  - Through customer's account (if an account is already created/used)
  - Mail
  - Electronically (if portable and in a readily usable format)

Deletion

- Requirements:
  - Delete customer's personal information from business records
  - Direct service providers to delete the customer's personal information from their records
- Exceptions
  - Transactional (i.e. current customer)
  - Security
  - Errors/Debug
  - Free Speech
  - CalECPA Compliance
  - Research in the Public Interest
  - Expected Internal Use
  - Legal Compliance
  - Other Internal Use

No Discrimination—Equal Services/Terms

- Business shall not:
  - Deny goods/services
  - Charge different price or rates
  - Provide different level or quality of goods/services
  - Suggest customer will receive different price/rate or level of goods/services
- How does this square with ability to offer financial incentive for collection of personal data?

Additional Business Obligations

- Training
  - "Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all of the requirements . . . and how to direct consumers to exercise their rights . . ."
- Service Provider Contracts
  - Contract requires specific language
  - Consider down-stream consequences if you are the service provider
- Operationalize all individual rights

Security Standards

- 1798.150. (a) (1) Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an 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*
- *"appropriate to the nature" = proportionality*

Bradley

Enforcement – Private Right of Action

- Currently only for violation of duty to maintain reasonable security coupled with a breach
- Statutory damages ($100-$750) per consumer
- But, currently a safe harbor:
  - Consumer must provide business notice identifying specific violations
  - If cured within 30 days and business provides consumer "an express written statement" violations have been cured – no action for individual statutory damages

Bradley

Enforcement – Attorney General

- Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General
  - *Includes "service provider, or other person"*
  - *Not limited to breach/security provision but any violation of the title*

Forthcoming AG Guidance

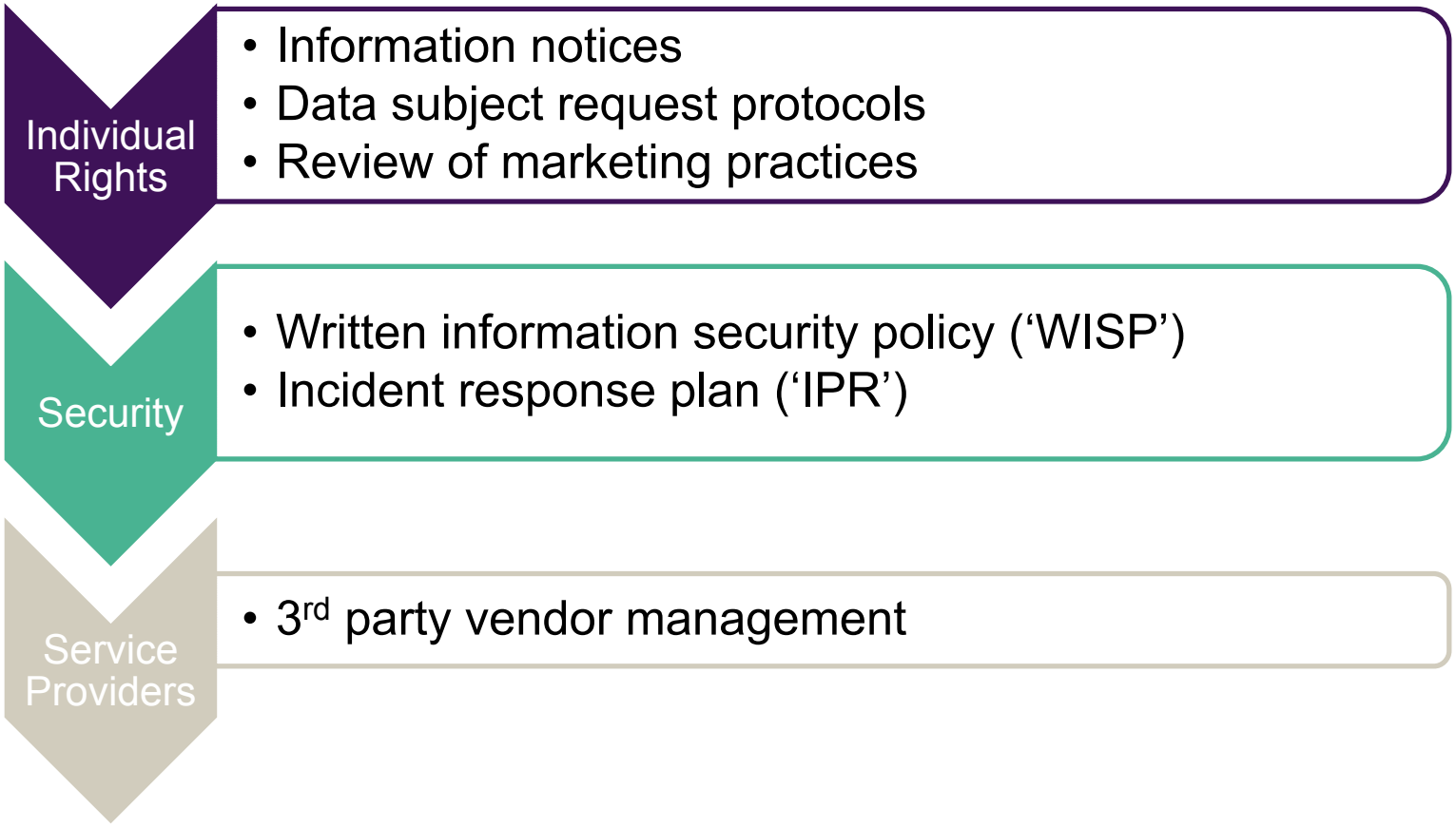
- On or before July 1, 2020, AG shall adopt regulations:
  - Categories of PI, definitions of unique identifiers
  - Any exceptions necessary regarding trade secrets, IP
  - Establish rules around:
    - Submission of opt-out request
    - Compliance with opt-out requests
    - Uniform opt-out logo or button
    - Notices are easily understood and available
    - Rules and procedures for consumer requests

Proposed Amendments

- Ten pending amendments to CCPA
  - Exemption for vehicle ownership information shared
  - Proposed amendment to the private and consumer enforcement mechanisms
  - Expand definition of publically available information to include any information lawfully made available from public records
  - Exempt employee from consumer definition
  - Amends definition of sell
  - Narrows definition of PI
  - Clarifies ability to use customer loyalty programs
  - Clarifies how requests must be made
  - Insurance exemption
- Six “other” privacy bills pending in California

Bradley

California Consumer Privacy Act--Considerations



Bradley

California Consumer Privacy Act

- Carve-Outs and Exemptions (Examples)
  - Gramm Leach Bliley Act (GLBA) and California Financial Information Privacy Act (CFIPA)
    - Exception for personal information collected, processed, sold, or disclosed pursuant to GLBA (does not apply to data breach obligations)
    - **Not Exempt:**
      - Employees, Business contacts, Commercial contacts
      - Customer prospects and leads
      - Website visitors
  - Opens the possibility that California will test financial services organizations on their GLBA and CFIPA compliance in order to determine if certain information falls within the exemption

California Consumer Privacy Act

- Carve-Outs and Exemptions
  - Clinical Trials
    - Exemption for personal information collected “as part of a clinical trial” if the clinical trial is subject to the Federal Policy for the Protection of Human Subjects
    - Other information may not be exempt:
      - Non-government funded clinical trial and research
      - Personal information collected not “as part of a clinical trial” such as eligibility determinations or referrals
      - Employee data

California Consumer Privacy Act

- Carve-Outs and Exemptions
  - HIPAA and CMIA
    - Exemption for PHI and MI, if:
      - Covered entity or Business Associate, (or provider of health care under CMIA and maintain on behalf of health care provider) and
      - PHI or MI
    - Other information may not be exempt
      - Marketing/Advertising
      - General communications
      - Employee data

CCPA—Compliance "To Do" List

- Identify personal information collection, use, and disclosure
- Determine purpose of each category of personal information
- Identify what personal information is disclosed to third parties
- Operationalize disclosures, deletion requests and do not sell obligations
- Privacy Notice and Website revisions
- Policies and Procedures
- Revise third-party service provider contracts
- Employee Training

Thank You!

Erin Jane Illman, CIPP/US
Board Certified Specialist in Privacy and Information Security Law
eillman@bradley.com
(704) 338-6026

Steve Snyder, CIPP/US, CIPT, FIP
Board Certified Specialist in Privacy and Information Security Law
ssnyder@bradley.com
(704) 338-6007

Bradley