Stradling

FOR THE ASSOCIATION OF CORPORATE COUNSEL, SOCAL CHAPTER

Privacy Law Update

CCPA 2.0, Virginia and Colorado

October 6, 2021

Presented by: Travis Brennan (Shareholder, Stradling)
Vanessa Novak (Corporate Counsel, Synoptek, LLC)

Change is Coming

- Nov. 3, 2020
  - CA voters enacted the California Privacy Rights Act (CPRA), which is a package of significant amendments to the CCPA
- Jan. 1, 2022
  - CPRA look-back period begins
- Jan. 1, 2023
  - CPRA, aka CCPA 2.0, takes effect
  - ***Virginia's*** Consumer Data Protection Act takes effect
- Jul. 1, 2023
  - ***Colorado*** Privacy Act takes effect.

A (Very) Brief CCPA Refresher

- First comprehensive consumer privacy law in the U.S. (Protects CA residents only)
- You're a regulated "business" (controller) if you do business in CA and: (i) your gross annual revenue is $25M+; or (ii) you annually collect the PI of 50,000+ CA residents, or (iii) 50%+ of revenue comes from sales of PI
- Businesses must disclose how they collect, use and share PI and respond to consumer requests
- Consumer rights to access (know), delete, or opt-out (of the "sale" of PI)
- AG's office can bring civil enforcement action for any violation (penalties up to $7,500 per violation) if violator does not cure
- Consumers may sue for security violations (if certain sensitive PI is involved); statutory damages up to $750 per person, per incident
- You're a regulated "service provider" (processor) if you process PI on behalf of a business under a contract that meets CCPA requirements

CCPA 2.0

New (Narrower?) Definition of a "Business"

CCPA

Do business in CA and:

(i) your gross annual revenue is $25M+; or

(ii) you annually collect the PI of 50,000+ CA residents, or

(iii) 50%+ of revenue comes from selling PI

CCPA 2.0

Do business in CA and:

(i) your gross annual revenue ***in the preceding calendar year*** is $25M+; or

(ii) you annually ***buy, sell or share*** the PI of ***100,000+*** CA residents, or

(iii) 50%+ of revenue comes from selling ***or sharing*** PI

More Consumer Rights

CCPA

Right to request:

- Access (know)
- Deletion
- Opt-out of sales of PI

CCPA 2.0

Right to request:

- Access (know)
- ***Correction***
- Deletion
- Opt-out of sales ***or "sharing"*** of PI

Right to limit use and disclosure of Sensitive PI

Sensitive PI

- SSN, driver’s license number, or other government-issued ID number
- Account login credentials
- Precise geolocation (radius of 1,850 feet or less)
- Racial or ethnic origin, religious or philosophical beliefs, union membership
- Content of mail, email or text messages (unless the business is the intended recipient)
- Genetic data
- Biometric data (e.g. facial recognition)
- Health information
- Sex life or sexual orientation

Selling vs. Sharing

Selling = 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 a third party for monetary or other valuable consideration**

Sharing = sharing, 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 a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration,** including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

More Requirements for "Service Provider" Contracts

CCPA

Service provider must agree not to:

(i) Sell PI

(ii) Use or disclose the PI for any purpose other than the business purpose in the agreement

(iii) Use or disclose the PI outside of the business relationship with the business

CCPA 2.0

Service provider must agree not to:

(i) Sell ***or Share*** PI

(ii) Use or disclose the PI for any purpose other than the business purpose in the agreement

(iii) Use or disclose the PI outside of the business relationship with the business

(iv) Combine PI with PI received from or on behalf of another person

New Agency With Expanded Enforcement Power

CCPA

- Enforced by CA AG
- Civil penalties may only be awarded by a court
- Guaranteed right to cure violations

CCPA 2.0

- ***Enforced by CA Privacy Protection Agency (CPPA)***
- **CPPA may impose administrative fines**
- ***No guaranteed right to cure violations***

Virginia Consumer Data Protection Act

Who is a Covered Controller (Business)?

Do business in VA, and:

- Control or process personal data of at least 100,000 consumers (VA residents) annually; or
- Control or process personal data of at least 25,000 consumers and derive more than 50% of gross revenue from the sale of personal data

Other Key Differences (Compared to CCPA 2.0)

- Clearer definition of “sale” = exchange of personal data for monetary consideration
- Opt-out right is broader. Consumer may opt out of:
  - Sales of PI;
  - Targeted advertising; or
  - Profiling
- Expressly exempts data collected in the “commercial” or “employment” context
- No private right of action
- More extensive contracting requirements for processors (service providers)

An Aside: Data Processing Agreements

- GDPR-driven, extra-territorial reach
- Origin of “controller” and “processor” framework
- In practice, DPAs take a variety of forms (clauses within service agreements, data processing “addendums,” or stand-alone agreements)
- Some common terms:
  - List of required security measures
  - Breach notification
  - Controller audit rights
  - Insurance coverage requirements
  - Limitations on liability

Colorado Privacy Act

Who is a Covered Controller (Business)?

Do business in CO, and:

- Control or process personal data of at least 100,000 consumers (CO residents) annually; or
- Derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data for 25,000 consumers or more

Other Key Differences (Compared to CCPA 2.0)

- Opt-out right is broader. Consumer may opt out of:
  - Sales of PI;
  - Targeted advertising; or
  - Profiling *via a universal opt-out mechanism*
- More extensive contracting requirements for processors (service providers)
- Definition of consumer expressly excludes individuals acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone in the employment context
- Guaranteed right to cure sunsets on January 1, 2025

Preparing For 2023 (And Beyond)

Practical Steps Toward Compliance With Current And Future Legal Frameworks

- Map your data
  - Define your relationship to different sources/categories of PI. Are you a business, service provider or both?
- Conduct a privacy audit (not the same as a security audit)
  - CCPA 2.0, VA and CO all impose data minimization obligations
  - Incorporate privacy controls into product/service development
  - Focus on advertising/marketing/re-targeting efforts
- Websites
  - Examine your use of cookies and trackers, and implement appropriate opt-out mechanisms
  - Consider implementing the “Global Privacy Control”
  - Consider clear and specific opt-in model for all non-essential cookies and trackers (GDPR style)

Practical Steps, cont.

- Mobile apps
  - Examine your use of SDKs and other third-party integrations, and make appropriate disclosures
- Harmonize service provider/processor contract provisions
  - If you're a service provider/processor, develop you own forms
  - Make limitations on liability clear
- Incorporate CIS Top 20 Controls into security assessments
- Cyber and privacy liability insurance
- Monitor the CA, VA and CO rulemaking processes

Questions?

Travis Brennan, tbrennan@stradlinglaw.com

Vanessa Novak, vnovak@synoptek.com