Stradling
Attorneys at Law

Data Privacy and Security Considerations for Contracts, Post-CCPA

May 21, 2020

Presented by:

Travis Brennan
Shareholder, Chair of Privacy & Data Security practice
tbrennan@sycr.com

CCPA Was Just The Beginning

- **1/1/2020** – CCPA in effect
- **??????** – CA Attorney General publishes final regulations
- **7/1/2020** – CCPA enforcement begins
- **11/3/2020** – California voters (probably) enact the California Privacy Rights Act of 2020 (CPRA), making significant changes to CCPA
- **??????** – More state (and federal?) privacy laws
- **1/1/2023** – CPRA changes take effect

Who are you?

- "Business" (Controller)
  - You collect consumers' (CA residents') PI, or it's collected on your behalf; you determine the purpose of processing; and you otherwise meet the act's definition of a Business ($25M in revenue OR collect PI of 50,000 consumers OR make at least 50% of revenue from selling PI)
  - You owe CCPA disclosures to consumers, and must process consumer requests to know/delete/opt-out
- "Service Provider" (Processor)
  - You collect or otherwise process the PI as part of a service you perform for the Business
  - Your agreement with Business prohibits you from using the PI for any purpose other than Business's, as required under Civ. Code s. 1798.140(2)(A).
  - You don't owe the disclosures to consumers, and may direct consumer requests you receive to the Business

Who are you? (cont.)

- You might be a Business in one context and a Service Provider in another
  - "A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells *outside of its role as a service provider*." Draft Reg. 999.314(f) (emphasis added).
    - *Practice tip*: This means your Privacy Policy doesn't have to describe how you collect, maintain or "sell" PI *in your role as a service provider*.
    - *Practice tip*: If you're a vendor, you might want to bind yourself to Service Provider restrictions regardless of whether your customer is a Business.
- "Third Party"
  - You receive PI from a Business but you're not a Business or Service Provider

Why It's Important To Get Service Provider Agreements Right

- From the Business's perspective:
  - Avoid committing a "Sale" of PI
    - "Sale" includes disclosing PI "to another business or a third party for monetary or other valuable consideration." Disclosure to a Service Provider is exempt.
  - Help fulfill duty to employ "reasonable security procedures and practices," which may reduce risk of consumer litigation and enforcement action in the event of a data breach.
- From the Service Provider's perspective:
  - Avoid becoming a Business (at least with respect to the PI at issue)
  - Limit scope of obligations under CCPA

Requirements for a Valid Service Provider Agreement

- Business must prohibit the vendor from:
  - Selling the PI
  - "retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the" agreement, "or as otherwise permitted by" the CCPA
  - "retaining, using, or disclosing the personal information outside of the direct business relationship" with the Business
- The vendor must "certify" that it understands these restrictions and will comply with them.
- Without these provisions, the Business is sharing with (and potentially Selling to) a Third Party, and the vendor is "collecting" the PI as a Third Party (or a Business)

Other Provisions To Consider

- Require Service Provider to extend restrictions to its own vendors/sub-contractors (CPRA)
- Require Service Provider to assist the Business in complying with consumer requests (CPRA)
- Require Service Provider to employ "reasonable security procedures and practices" (CPRA)
  - Consumers can sue for a breach of sensitive PI, and get statutory damages up to $750 "per consumer per incident," if the breach is "a result of ***the business's*** violation of the duty to implement and maintain reasonable security procedures and practices." Civ. Code s. 1798.150(a)(1) (emphasis added).
  - What's reasonable security? Start with CIS Top 20 Critical Security Controls.

Other Provisions to Consider (cont.)

- Require Service Provider to submit to regular security and compliance audits (CPRA)
- Limitations on liability
  - The CCPA provides that a Business shall not be liable for violations of its Service provider (and vice versa), unless it had reason to know the violation would occur. Civ. Code. s. 1798.145(j).
  - Consider rep and warranty that the Business/Service provider willy comply.
- Indemnity for third party claims
  - Carefully define "Claim" and "Losses." Include actions by regulators and fines/penalties?
  - Specify rights regarding appointment of defense counsel, control of litigation and settlement of Claims
  - Dollar amount cap?

Other Provisions to Consider (cont.)

- Insurance
  - Require cyber and privacy liability coverage?
  - Require Service Provider to designate Business as additional insured?

Agreements With Third Parties

- A Third Party is anyone you share PI with that is not subject to the Service Provider restrictions on use and disclosure
- If you're the Business, consider:
  - Requiring the Third Party to abide by consumer requests you receive, particularly requests to opt-out (if applicable)
  - Requiring the Third Party to comply with CCPA privacy protections (CPRA)
  - Requiring the Third Party to employ reasonable security procedures and practices
  - Will the relationship involving "Sharing" PI as defined under CPRA?
    - Sharing = sharing "by the business to a third party for cross-context behavioral advertising"

Agreements With Third Parties (cont.)

- If you're the Third Party, consider:
  - requiring the Business to represent/warrant that consumer PI it shares with you was collected in compliance with CCPA and other applicable laws, especially if you intend to "resell" the PI
    - "A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out." Civ. Code s. 1798.115(d).

Stradling
Attorneys at Law

Questions?