# Does the CCPA as modified by the CPRA apply to your business?

By Jennifer Sheridan, CIPP/E, CIPP/US

March 10, 2023

*Originally published by The International Association of Privacy Professionals*

The California Consumer Protection Act has been in effect since Jan. 1, 2020 and the California Privacy Rights Act, which modified the CCPA, went into effect Jan. 1, 2023.

Now that the CPRA is in effect, one of the questions businesses are concerned about is the modification of the CCPA threshold test of "what is a business," and the implications this modification for small businesses, e.g., those under USD25 million in annual revenue, in light of the new compliance requirements for business-to-business and employee personal information.

Unlike the EU or U.K. General Data Protection Regulations, not all businesses must comply with the CCPA. Nonprofits are carved out of the CCPA, where they are covered under the GDPR. The line defining small businesses is less clear. The CCPA was structured with a three-part threshold test for determining whether compliance was required. If a business qualifies under any of the three parts, then it must comply with the statute.

The seemingly easier parts to solve are the revenue and data broker thresholds. If a business has more than USD25 million in annual revenue or receives 50% or more of its revenue from the sale of personal information, usually these are referred to as data brokers, then it is covered by the CCPA.

The third threshold concerns the number, or "count," of personal information records related to the business. This is where the analysis is more complex.

Below are the two versions of this threshold:

The original CCPA version, effective before Jan. 1, read: "(B) Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices" per California Civil Code 1798.140.

The CPRA-modified version of the CCPA, effective Jan. 1, reads: "(B) Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households" per Cal. Civ. Code 1798.140.

In October 2019, I coauthored the article, CCPA myth buster: Not all records count, which analyzed the original CCPA threshold and questioned whether commercial purposes were coextensive with business purposes. Commentators had conflated "business" and "commercial" purpose such that most for-profit websites were considered covered by the CCPA. My coauthor and I took a narrower view of this definition than most commentators.

The CPRA-modified version of the CCPA has deleted any reference to commercial or business purpose, as well as the reference to "receive" in the threshold test of a business based on personal information record count. The revised test is whether the business buys, sells or shares personal information.

This new definition of "what is a business" invites the question: Could a small business that does not meet the USD25 million revenue threshold, is not a data broker as defined in the statute and not engaged in targeted advertising as defined in the statute, take the position that the CPRA-modified version of the CCPA does not apply to their business?

As of Jan. 1, business-to-business and employee personal information are included as part of the CPRA-modified version of the CCPA creating a significant increase in compliance requirements, especially for small companies.

California is an outlier in the U.S., as these types of personal information are exempted from the four new privacy laws in Virginia, Colorado, Connecticut and Utah.

For small businesses with less than USD25 million in annual revenue, this interpretation could mean a significant reduction in costs and resources. Of course, a business must conduct the appropriate analysis to determine it does not meet any of three thresholds of "what is a business" under the CPRA before deciding the CCPA, as modified by CPRA, does not apply to their business.

WEBINAR



# CPRA & the 2023 Alphabet Soup of US Privacy Regulations

Jennifer ("Jenny") Sheridan, Principal, JLSheridan Law

Megan Kelly, Director of Attorney Development, Paragon Legal

May 19, 2023

# BACKGROUND

- Started as corporate attorney – wall street NYC law firm; palo alto corporate firm.
- In-house counsel for several Silicon Valley tech companies.
- Headed WW licensing team for BEA Systems (now part of Oracle).
- GC privately held and publicly traded software companies.
- Teaching law as adjunct at Santa Clara Law and USF Law, as well as visiting full-time at Drexel Law School.
- Founded JLSheridan Law boutique firm focused on tech transactions, privacy compliance, and IP counseling in 2014.
- Certified IAPP privacy professional with the CIPP/US and CIPP/E certifications.

# TODAY'S TOPICS

*How does CCPA (modified by CPRA) affect a typical B2B SaaS company?*

* What is required with the expiration of the B2B and employee exemptions in January 2023?
* What are the new requirements for Service Provider agreements?
* What is the new purpose limitation and what do companies need to do to be in compliance?
* What is sensitive data category?
* What are impact assessments?
* What is automated decision making?

High level overview/comparison with other US state privacy laws: VA, Colorado, CT and Utah.

# GDPR IS COMING TO THE US

- Terminology: most of the new US privacy laws (except CA) use GDPR terms like data controller, data processor, data subject, personal data.
- "Risk assessment" "Impact Assessment" – all similar to GDPR's DPIA – data protection impact assessment.
- Privacy principles such as "privacy by design," "data minimization," "purpose limitation," "automated decision making," "profiling," "dark patterns" are being referenced in the upcoming 2023 US privacy laws.
- Opt-in consent similar to GDPR (VA, Colorado, CT) – freely given (thus revocable), specific, informed, and unambiguous.

# WHAT'S NOT BEING COVERING

- Global Privacy Control (AG settlement with Sephora under CCPA).
- Adtech compliance.

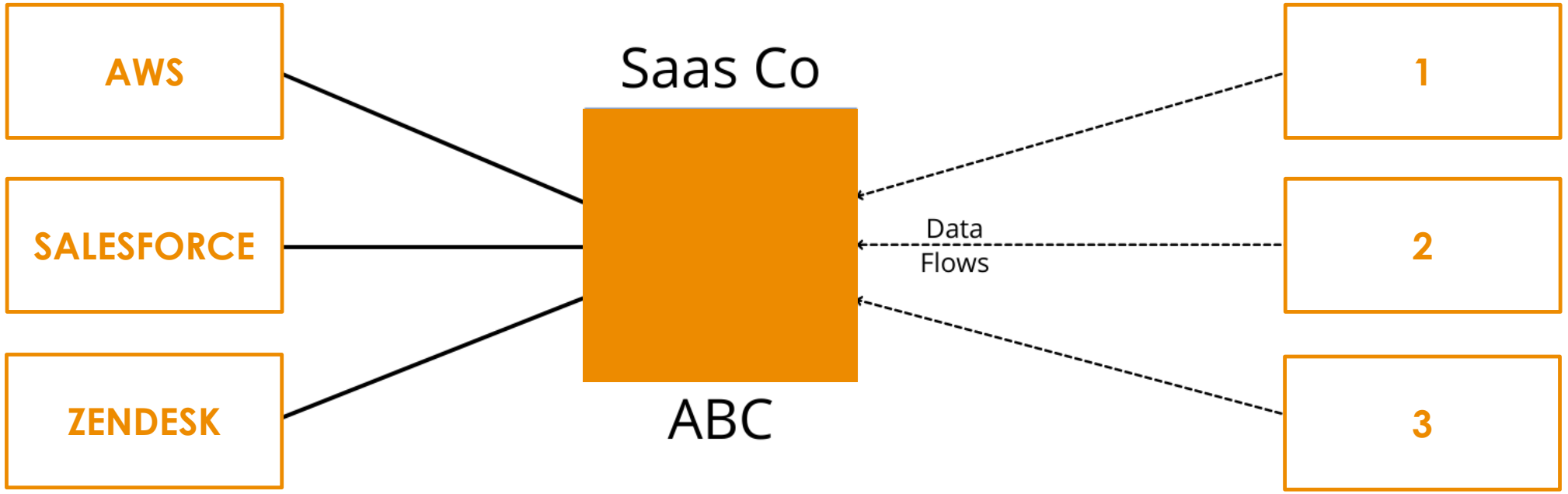
# B2B USE CASE

- **ABC Corp is a SaaS company** ("B2B"). Its platform provides enterprise customers an all-in-one project management solution. Services are provided on an annual subscription basis. Its customers are in the EU, the UK, and the US. The platform users are the enterprise customer's employees and/or customers.
- It has a CCPA compliant privacy policy.
- What does it need to do to be compliant with CPRA (amends CCPA) and the new 2023 US state privacy laws: VA, Colorado, CT and Utah?
- It needs to review its data flows.

# B2B Personal Data Flows

Service Providers / Data Processors

Enterprise Customers 1, 2 & 3




| | | GDPR | | CCPA |
|---|---|---|---|---|
| SaaS Co | = | Data Processor | = | Service Provider |
| Customer | = | Data Controller | = | Covered Business |
| AWS | = | Subprocessor | = | Service Provider |

Types of Personal Data:

- Name
- Email
- IP Addresses

# NEW CONSUMER RIGHTS UNDER CPRA

1. B2B & employee info rights: CCPA had a moratorium on these categories that expires January 2023. (cf. other US state privacy laws.). Discuss what ABC did for CCPA compliance as B2B company (compared to B2C).

2. Right to Correct Information: A consumer has the right to request that a business correct any inaccurate personal information.

3. Right to Limit Use and Disclosure of Sensitive PI: A consumer has the right to limit the use and disclosure of their SPI to that "use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods and services."

4. Right to Access Information About Automated Decision Making & Right to Opt-Out of ADM: A consumer has the right to request "meaningful information about the logic involved in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer."

# CPRA (CA) SENSITIVE INFORMATION DEFINITION

**1) govt IDs (e.g. SS, driver's license, passport);**

**2) consumer log-in, financial account, debit/credit # + required security/access code allowing access;**

3) precise geolocation;

4) racial/ethnic origin, religious, philosophical, union membership;

**5) consumer's email content UNLESS business intended recipient;**

6) Genetic data;

7) Biometric data;

8) Health data & sex life/sex orientation data.

# CPRA (CA) SENSITIVE INFORMATION OBLIGATIONS

- Opt-out right: Company must give the consumer the right to limit the use of its sensitive information UNLESS it is necessary to provide the products or services, e.g. consumer requests genetic testing.
- Opt-in right:  Virgina, Colorado and CT require opt-in defining consent similarly to GDPR – freely given, specific, informed, unambiguous.
- CA has a few more categories than other states (VA, Colorado, Utah, CT) but it does not have personal information of known child that some other states include in sensitive information category.

# CPRA "RISK ASSESSMENTS"

- CPRA's "risk assessments" will be required for companies whose processing activities present "significant risk" to consumers' privacy or security. What is 'significant risk'? TBD in upcoming rulemaking by the CA Privacy Protection Agency.
- A "risk assessment" required under the CPRA must:
- indicate whether the processing involves sensitive personal information, and
- identify and **weigh the benefits** resulting from the processing to the business, the consumer, other stakeholders, and the public, against the **potential risks** to the rights of the consumer associated with such processing, with the goal of restricting or prohibiting such processing if the risks to the privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.
- Compare GDPR's DPIA and legitimate interests assessment.

# IMPACT (OR "RISK") ASSESSMENT REQUIREMENT IN OTHER STATES

- VA, Colorado and CT all require impact assessments for 'high risk' processing.
- Identified types of 'high risk' processing:
- (i) targeted advertising;
- (ii) sale of personal information/personal data;
- (iii) sensitive data;
- (iv) profiling.

# AUTOMATED DECISION MAKING ("ADM"): NEW OPT-OUT RIGHTS

- CPRA (CA) charges the CA Privacy Protection Agency with adopting regulations "governing access and opt-out rights with respect to businesses' use of automated decision making technology," including providing meaningful information about the logic of the decision and the likely outcome with respect to the consumer.
- Note: CPPA's mandate is not limited to 'solely' automated decision (e.g. without human involvement) or those with 'legal effects.'
- VA, Colorado and CT have similar provisions.
- Note: All of these new laws will require companies processing personal information using ADM to conduct "risk assessments."

# CPRA (CCPA AMENDED): AS OF JAN '23 (ENFORCEMENT JULY '23)

- Employees: privacy notices to employees is required similar to consumers. Most companies will add these disclosures in the employee manual (not public facing site);
- B2B personal information: B2B contacts will have same rights of access, deletion, etc. as B2C under CCPA. Privacy Policy needs to be updated.
- Note: CA will be the only US state including employee and B2B personal information.
- Evaluate if need to add the "DNSellMPI" or "DNShareMPI" button.
- Evaluate if processing any sensitive personal information that would require "opt-out" or "opt-in."
- Evaluate whether its processing is 'high risk' and requires a DPIA (or similar impact assessment).

# CALIFORNIA PRIVACY PROTECTION AGENCY (CPPA)

- CPPA still to issue draft regs on certain topics including including ADM and risk assessments (Part II regs).
- Part I of the regs has been finalized.
- Part II of the regs is still pending. California Privacy Protection Agency has taken comments from the public but has not yet issued draft (or final) regulations.
- Sign up to receive messages from CA Privacy Protection Agency: https://cppa.ca.gov/about_us/contact.html
- Recent CPPA regs: https://cppa.ca.gov/meetings/materials/20221021_22.html

# THANK YOU!



**Paragon Legal**

Website: https://paragonlegal.com

Email: info@paragonlegal.com

**Jennifer (Jenny) Lynn Sheridan, Esquire**
**Principal, JLSheridan Law**

Email: jenny@jlsheridan.legal

Website: https://www.jlsheridan.legal

LinkedIn: https://www.linkedin.com/in/jenny-lynn-sheridan-cipp-us-aba6843