



SESSION ONE: CALIFORNIA AND CHINA - TWO WORLDVIEWS ON DATA PRIVACY | FEBRUARY 2022

So, What is the California Privacy Rights Act (CPRA) all About?

- November 2020 ballot initiative that expands upon the California Consumer Privacy Act (CCPA) – provides for even greater rights for consumers to prevent businesses from sharing their personal data, correct inaccurate personal data, and limit businesses' usage of sensitive personal information.
- It creates a dedicated agency – the California Privacy Protection Agency (CPPA) – to implement and enforce state privacy laws, investigate violations, and assess penalties.
- The CPRA will take effect on Jan. 1, 2023, and apply to personal data collected on or after Jan.1, 2022.
- It expands privacy protections to employees and independent contractors.

Several Broad Definitions to Understand

- **Personal Information:** Any "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Publicly available information and deidentified or aggregated consumer information are excluded from the definition.
- New separately defined "sensitive information" category.
- Includes Human Resources information of employees, applicants, independent contractors, etc.
- **Consumer** is defined as "a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, however identified, including by a unique identifier."
- The CPRA does not change this definition.
- **18 CCR § 17014 defines "resident" to include:**
 - Every individual who is in the state for other than a temporary or transitory purpose; and
 - Every individual who is domiciled in the state who is outside the state for a temporary or transitory purpose.

"Sale" of Personal Information

- Under the CCPA, the term "sell" means "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating ... a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."
- This definition excludes certain transactions, including when a business uses or shares a consumer's personal information with a service provider if certain conditions are met.
- The CPRA revises the exclusions provided under the definition and removes the carve-out for transactions with service providers.

"Sharing" Personal Information

- New under the CPRA.
- Applies when businesses disclose information for cross-context behavioral advertising, "whether or not for monetary or other valuable consideration."

Special Treatment of Sensitive Personal Info: "Sensitive Personal Information" is a new Definition in CPRA

- Examples: "Government ID, finances, geolocation, race, religion, union membership, communications, genetics, biometrics, health and sexual orientation."
 - This information is particularly prevalent in the employment context.

China's Personal Information Protection Law (PIPL)

Why does it matter?

- Although similar to the General Data Protection Regulation (GDPR) in some ways, PIPL is even more strict than the CCPA/CPRA or even the GDPR.
- Imposes a higher compliance burden than any other global data protection law.
- China's PIPL takes a stand against transfer of Chinese personal data out of the country.
- The PIPL contemplates much more significant and frequent government oversight of personal data processing.
- Significant fines are possible against "responsible persons," for minor violations, ranging from CN¥10,000 to ¥100,000. (Approx. \$1,572-\$15,721).
- For major violations, China may impose fines up to 5% of global revenue or ¥50 million (\$7.8 million).
- China also has the authority to issue orders to suspend or terminate personal data processing.
- Went into effect Nov. 1, 2021.

But new Themes Emerge

- But the PIPL is more extensive than other laws.
- Data "processors" must be "supervised."
- Disclosures must address "methods" of processing as well as purposes.
- Transfers outside the country are permitted only when "genuinely needed."
- Organizations processing relatively small quantities of personal data may not be able to transfer data outside the country.
- Many organizations who wish to transfer data outside of China will need to undergo an assessment from China's cybersecurity agency.

We Should be Familiar with Some of the Themes

PIPL shares many features with GDPR and other global privacy laws:

- Wide territorial scope.
- Principles of necessity/proportionality, transparency, accuracy, and fairness.
- Requirements for appropriate security.
- A legal basis to legitimize processing.
- Special requirements for sensitive data and automated decision making.
- Rules for entrusting personal data to "processors."
- Recordkeeping requirements.
- Rules to protect data passing outside national borders.

Responses to California and China

- **Educating** critical stakeholders throughout the organization about the CPRA/PIPL.
- **Appointing** key personal data gatekeepers throughout the different functional areas of your organization.
- **Identifying** material data assets and primary data channels.
- **Cataloguing** and analyzing data processing activities (for purposes of ensuring they all have a lawful basis).
- **Analyzing** how notice and consent are currently being given and obtained.
- **Preparing** a data breach response plan and team.
- **Revising** procedures and processes to accommodate individual rights requests.
- **Identifying** and revising third-party vendor data processing relationships and contracts.
- **Determining** your organization's legitimate bases for processing information.
- **Implementing** data transfer mechanisms as necessary.

ARMSTRONG TEASDALE'S PRIVACY AND DATA SECURITY TEAM



Jeffrey Schultz

ST. LOUIS | PARTNER

jschultz@atllp.com
314.259.4732



Scott Galt

ST. LOUIS | PARTNER

sgalt@atllp.com
314.259.4709



Romaine Marshall

SALT LAKE CITY | PARTNER

rmarshall@atllp.com
801.401.1604



Daniella Gordon

PHILADELPHIA | PARTNER

dgordon@atllp.com
267.780.2017



Francisco Villegas

NEW YORK | PARTNER

fvillegas@atllp.com
212.209.4436



Zane Shihab

LONDON | PARTNER

zshihab@atllp.co.uk
+44 20 7539 7312



Lucas Amodio

ST. LOUIS | PARTNER

lamodio@atllp.com
314.259.4722



Dustin Berger

DENVER | SENIOR ASSOCIATE

dberger@atllp.com
720.722.7197



Casey Waughn

ST. LOUIS | ASSOCIATE

cwaughn@atllp.com
314.259.4766



Caitlin Fagan

ST. LOUIS | ASSOCIATE

cfagan@atllp.com
314.259.4781



Ryan Smith

PHILADELPHIA | ASSOCIATE

rasmith@atllp.com
267.780.2070



Gabriela Baeza-Stout

ST. LOUIS | ASSOCIATE

gbaezastout@atllp.com
314.386.6871



Jared Keetch

SALT LAKE CITY | ASSOCIATE

jkeetch@atllp.com
801.401.1615



Emily Nuvan

SALT LAKE CITY | ASSOCIATE

enuvan@atllp.com
801.401.1603



Nicole Polzin

KANSAS CITY | ASSOCIATE

npolzin@atllp.com
816.472.3105