# California Privacy Rights Act of 2020 (CCPA 2.0)

Maureen Dry-Wasson, VP-Group General Counsel and
Global Privacy Officer, Allegis Group, Inc.
Cris Potter, Chief Ethics and Privacy Officer, SAIC
April Falcon Doss, Saul Ewing Arnstein & Lehr

SAUL EWING
ARNSTEIN
& LEHR LLP

# How did the CPRA come to be?

- CPRA is the second consumer privacy ballot initiative from Californians for Consumer Privacy, a non-profit led by Alastair Mactaggart

- Mactaggart's organization introduced the CPRA ballot initiative on November 13, 2019 in response to concerns that the 2019 legislative amendment process weakened the privacy protections in the California Consumer Privacy Act (CCPA)

SAUL EWING ARNSTEIN & LEHR LLP

# What is the status of CPRA?

- Californians for Consumer Privacy submitted over 900,000 signatures in support of the CPRA on May 4, 2020
- On Nov. 3, California voters approved the measure (vote to be certified after Nov. 20th)
- CPRA's text limits the legislature's ability to amend the law

# What does CPRA do?

- Creates the California Privacy Protection Agency
  - Funding and agency establishment shortly after vote certification – as early as Dec. 2020
  - Rulemaking to begin as early as July 2021
- New Rights to Consumers
  - Right to restrict use of sensitive personal information, including geolocation
  - Right to correct personal information
  - Right to opt out of data "sharing"
  - Data minimization and purpose limitation
  - Right to opt out of advertisers using precise geolocation information

# What does CPRA do?

- New Obligations for Businesses
  - Updated disclosures
  - Offline mechanisms for opt-out
  - No disclosure (Sale or Sharing) without a governing contract
  - Retention limits
  - “Reasonable security” obligations
  - Security audit for certain business activities
  - Expanded scope of private right of action

# What does CPRA do?

- Definitions and New Concepts
  - Business – modification to threshold
  - CCPA definition:
    - Annual gross revenue of $25 million; OR
    - Sell or share for commercial purposes the personal information of 50,000 or more California residents, households, or devices; OR
    - Derive 50 percent or more of its annual revenue from selling the personal information of California residents
  - CPRA increases threshold from 50,000 to 100,000 CA consumers, and added joint venture or partnership

# What does CPRA do?

- Definitions and New Concepts
  - Business purpose
    - Under CCPA a transfer of personal information is not a "sale" when a business uses or shares with a service provider personal information of a consumer that is **necessary to perform a business purpose** if conditions are met
  - CPRA makes significant changes to the definition of "business purpose" that would affect the activities service providers or contractors would be able to undertake outside the definitions of "sale" or "sharing."

# What does CPRA do?

- Definitions and New Concepts
  - Precise geolocation
  - Non-personalized advertising
    - ***Non-personalized advertising*** based on a consumer's current interaction with a business ***is a business purpose***.
    - Definition: "advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business, **with the exception of the consumer's precise geolocation**."
  - Precise geolocation
    - "data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet, except as prescribed by regulations."

# What does CPRA do?

- Definitions and New Concepts
  - CPRA makes explicit that "advertising and marketing services" are business purposes except for cross-context behavioral advertising
  - "Cross-context behavioral advertising" is a new defined term meaning "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."

SAUL EWING ARNSTEIN & LEHR LLP

# What does CPRA do?

- Definitions and New Concepts
  - Sensitive personal information
    - Sensitive personal information includes ID numbers, account details, location data, diversity data, mail content, genetic data, biological data
    - Consumers can opt out of use, not just sale
  - Security and integrity
    - The CPRA creates a requirement for reasonable security measures: “A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal Information from unauthorized or illegal access, destruction, use, modification, or disclosure[.]”

# Implementation Timeline

- January 1, 2023 - Two year ramp-up before law takes full effect
- The current B2B and employee exemptions in CCPA are extended until January 1, 2023
- Rulemaking timeline
  - July 1, 2021 – new California Privacy Protection Agency will begin rulemaking process
  - July 1, 2022 – final date for agency to adopt regulations
  - January 1, 2023 – fully operative
  - July 1, 2023 – enforcement date

# Implementation Planning

- For companies subject to CCPA and CPRA, what's next?
- Key industry considerations
  - B2B industries
  - Consumer-data-intensive industries
- Key timing considerations
  - Applicable to data acquired after Jan. 1, 2022

# Implementation Planning

- This is a good time to assess:
  - Threshold if not covered by CCPA
  - Sensitive data
  - Data retention practices
  - Security posture
  - Data sharing with digital advertising partners
- This is a good time to update:
  - Procedures for responding to consumer requests
  - Website privacy policies and other privacy notices
  - Website links

SAUL EWING ARNSTEIN & LEHR LLP

# CPRA Summary of Key Provisions

1. Sensitive Data
2. New Enforcement Agency
3. Expanded Breach Liability
4. Audits and Risk Assessments
5. Automated Decision-Making and Profiling
6. Data Correction
7. Children's Data
8. Data Retention
9. Employee Data
10. Service Provider/ Contractor/ Third Party

SAUL EWING
ARNSTEIN
& LEHR LLP

# Tackling Real Life Privacy Compliance Challenges - Strategy

- Privacy principles approach – finding commonality across privacy laws
- Strong regional personnel (North America, EMEA, APAC) with global coordination
- Personnel embedded in business units (full-time committed to privacy/security with privacy certifications) with strategy set by corporate Global Privacy Office
- Strong alliances with primary stakeholders (IS, Info Sec, Data Governance)
- Strong partnerships with other key stakeholder groups:
  - HR
  - Marketing
  - Sales
  - Strategic Development/M&A
  - Legal
  - Compliance/Risk
  - Finance
  - Communications
  - Procurement
- Formation of Data Protection Oversight Committee
- IAPP Sponsorship
- Training and Awareness




SAUL EWING ARNSTEIN & LEHR LLP

# Data Protection Oversight Committee

- **What does it do?**
  - Forum to discuss privacy initiatives and problem solve risks to the business

- **Who is on it? – Senior Leaders of the following functions:**
  - Privacy
  - Information Security
  - Data Governance
  - Finance
  - Legal
  - Risk/Compliance/Insurance
  - HR
  - IS/IT
  - Strategic Development/M&A
  - Sales
  - Marketing
  - Guests: Business Unit Privacy Analysts (rotated each meeting)

- **How often does it meet?**
  - Monthly initially and once established quarterly to 3 times per year
- **Who sets the agenda?**
  - Agenda set through a pre-meeting between leaders of Privacy, Info Sec, and the Privacy and Protection Team within IS

SAUL EWING ARNSTEIN & LEHR LLP

# Key Roles to Support Global Privacy Office

In addition to the privacy practitioners in the Global Privacy Office, it is helpful to have IS or some other department devote personnel resources in the following roles to assist and support the Global Privacy Office:

- **Privacy Architect (to help with Privacy by Design)**
- **Records Retention/Records Manager (to help with records retention/data minimization issues)**
- **Strategic Change Management (to assist with behavior/process change)**
- **Business Process Analysts (to study current state and identify gaps)**
- **IS Product Owners (to be responsible for technology the Privacy Office may adopt)**
- **IS Project Managers (to manage the various IS initiatives tied to Privacy)**

# Privacy Liaisons/Champions/Ambassadors

- **Who are they?**
  - Employees who support the Privacy Office and other privacy functions to help drive safe and effective privacy practices.
  - They have another full-time role but are willing to devote a reasonable time commitment to help support the Privacy Office.

- **What do they do?**
  - ✓ Develop a level of understanding of privacy issues that is higher than the average employee.
  - ✓ Understand their department's business activities and how personal data is involved with them.
  - ✓ Receive communications from the Privacy Office related to Privacy Office initiatives and help disseminate and support this information with their teams.
  - ✓ Refer privacy-related questions or concerns to the appropriate personnel at the Privacy Office as necessary.
  - ✓ Be educated on how to report a privacy incident and assist members of their team, as needed, to report privacy incidents.

- **How does the Privacy Office support them?**
  - By assigning additional online trainings or other trainings and sending pertinent articles or other reading materials.
  - Providing access to the company's online privacy research tools.

SAUL EWING ARNSTEIN & LEHR LLP

# Top Ten Data Protection Readiness Initiatives

- ❑ Understanding our Data – Data Mapping/Data Inventory
- ❑ Data Breach Reporting/Incident Response
- ❑ Data Protection Contract Language – Customers and Suppliers
- ❑ Training and Awareness/Appointment of DPO (where required)
- ❑ Data Subject Rights
- ❑ Data Transfers (not a concern under CPRA)
- ❑ Data Minimization
- ❑ Information Security
- ❑ Privacy in Day-to-Day Operations/Privacy by Design/DPIAs and PIAs
- ❑ Privacy Notices




SAUL EWING ARNSTEIN & LEHR LLP

# Questions



SAUL EWING
ARNSTEIN
& LEHR LLP