CALIFORNIA PRIVACY RIGHTS ACT (CPRA)

WHAT BUSINESSES FACE UNDER CALIFORNIA’S EXPANDED PRIVACY LAW & HOW YOU CAN PREPARE NOW
SPEAKERS

MIKE MORGAN
Partner
Los Angeles
+1 310 551 9366
mmorgan@mwe.com

JESSICA MCGAHIE SAWYER
Counsel
Los Angeles
+1 310 551 9397
jsawyer@mwe.com

WENDY ZHANG
Associate
Los Angeles
+1 310 788 6012
wwzhang@mwe.com
AGENDA

• How We Got Here

• Key Changes Under CPRA

• Enforcement & Creation of the CPRA

• Expanded Cybersecurity Obligations

• Practical Steps to Review CCPA Compliance & Prepare for CPRA
The California Privacy Rights Act (CPRA) – newly approved ballot initiative (Prop 24) amending the California Consumer Privacy Act (CCPA)

• The CCPA currently requires:
  – Data Subject Rights – individuals can access and delete their data
  – Statutory damages for data breaches
  – Special obligations and opt out rights applicable to data “sellers”
  – Service provider contracting
  – Detailed privacy policies and other notices for broadly-defined “personal information”
HOW WE GOT HERE (CONT.)

• CPRA proposed by the same backers as CCPA, despite significant CCPA undertakings:
  – Estimated $50B in compliance costs from the CCPA alone (Compliance Week)
  – California AG produced detailed regulations, hundreds of pages of guidance
  – Legislature considered dozens of amendments

Good news: CPRA not effective until January 1, 2023*
CCPA ENFORCEMENT THUS FAR

- CCPA provides for enforcement by the California Attorney General and a private right of action in certain circumstances
  - Statutory damages amount up to $750 per violation
- Swift enforcement by California Attorney General
  - Several notices of noncompliance sent to businesses across sectors starting July 1, 2020
- Class actions and multi-district litigation
  - November 2020 class action settlement under CCPA - $400,000
CCPA ENFORCEMENT THUS FAR (CONT.)

• Approximately **50 private right of action cases** filed since January 1, 2020
  – Centered around **data breaches**
  – **Pushing the reach and scope** of the private right of action
    ▪ Some lawsuits based on lack of notice, no-opt out, and retroactive application
    ▪ **Attempted application to non-CA resident** who spent time in a CA treatment facility
KEY CHANGES UNDER CPRA
NEW RIGHTS: “SHARING” OPT-OUT

CCPA regulated “sales” of personal information. CPRA expands to “sharing” for “cross-context behavioral advertising,” defined:

• “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”

• Resolves questions about whether ad tech uses are “sales” under CCPA

• Expands opt out rights to buy side advertising previously exempt from “sale” obligations

Most practices colloquially considered “sharing” not affected—only applies to targeted advertising

NEW CONSUMER RIGHTS

1. Opt out of data “sharing”
2. Limit sensitive information
3. Correct inaccurate information
NEW RIGHTS: SENSITIVE INFORMATION

Sensitive personal information includes:

- Traditional “PII” categories: Government ID, financial account/card numbers, account login information
- Parallels GDPR “special categories”:
  - Racial or ethnic origin, religious or philosophical beliefs
  - Union membership, biometric information, health information
  - Sex life/orientation
- Other sensitive categories:
  - Genetic data
  - Precise geolocation information
  - Communications content

Does not include information that is processed “without the purpose of inferring characteristics about a consumer”
NEW RIGHTS: SENSITIVE INFORMATION

Businesses that process sensitive personal information must allow consumers right to limit processing to certain purposes:

- Security and integrity
- Short term, transient use
- “Services on behalf of the business” including storage, account service, payment processing/fulfillment
- Verify/maintain quality or security of service or “improve” same

If used for any other purpose, businesses must provide right via link on homepage: “Limit the Use of My Sensitive Personal Information”

- Mirrors “sale” opt out right, but applicable to more businesses

NEW CONSUMER RIGHTS

1. Opt out of data “sharing”
2. Limit sensitive information
3. Correct inaccurate information
NEW RIGHTS: DATA CORRECTION

Data subjects currently have access (including portability) and deletion rights. CPRA expands to include correction of inaccurate data.

• Introduces operational difficulties
  – How should businesses confirm that data is “inaccurate”?
  – Service provider/data recipient issues
NEW DATA COLLECTION AND RETENTION REQUIREMENTS

• New broad obligation for businesses to collect/use data only as “reasonably necessary and proportionate to achieve the purposes” of collection
  – No secondary use unless “compatible with the context”

• Important new data retention requirements: data may only be retained as long as “reasonably necessary,” disclose retention schedules/criteria in privacy policies

• Wait and see on rulemaking
NEW PRIVACY NOTICE REQUIREMENTS

Companies will need to update privacy notices

• Include information data “sharing” and “sensitive personal data” processing, if any
• Categories of sources from which consumers’ personal information is collected, and categories of third parties to whom disclosed
• “Business or commercial purpose for collecting or selling or sharing consumers’ personal information”
• Data retention - criteria or specific timeframe
UPDATES TO PRIVACY CONTRACTING

- Many changes, little clarity
- CCPA had contracting requirements for “service providers” and “third party exemption” entities
- CPRA introduces new “contractor” category, replacing “third party exemption”
- New contract terms (in addition to previous service provider terms):
  - Specific purposes
  - Compliance with law
  - Pass on requirements
  - Audit/Accountability rights
  - Notice of noncompliance and right of remediation
- Service providers and contractors expressly subject to CPRA enforcement
- Contracts also required for data partners: recipients of data “sales” or “shares”
- Will lead to more confusion and battle-of-the-forms between companies
CHANGES TO EMPLOYEE / B2B DATA EXEMPTION

• CPRA extends employee and B2B exemptions until 2023

• **Employee exemption**
  – Includes independent contractors, job applicants
  – Data must be used in the context of employment

• **B2B exemption**
  – Somewhat limited – applies to data involved in a communication related to a transaction.
  – Does not apply to data obtained from third parties (e.g., purchasing marketing lists from business contacts)
  – Does not apply to data sales

• Further developments likely
ENFORCEMENT & CREATION OF THE CALIFORNIA PRIVACY PROTECTION AGENCY (CPPA)
REGULATIONS AND ENFORCEMENT

• CPRA creates and funds new privacy enforcement agency, California Privacy Protection Agency (CPPA) – most powerful US privacy regulator

• Expansive rulemaking authority, including to create new rights, regulate “high risk” data businesses
  – Additional rights: automated decision-making/“profiling” access and opt out
  – High risk businesses – annual risk assessments submitted to agency

• Potentially large administrative fines go to “offset” enforcement costs
  – Tripled fines for data concerning minors

• Additional AG and local government enforcement
  – Removes 30-day cure period for regulatory enforcement

• Private right of action
EXPANDED CYBERSECURITY OBLIGATIONS
INCREASED CYBERSECURITY OBLIGATIONS

• Expansion of private right of action for data breaches
  – Under CCPA, only applied to breaches of “traditional” PII
  – Now includes account/password combinations
  – Limited cure period

• New “reasonable security” duty for all personal information
  – Can be enforced without the occurrence of a data breach

• Private actions brought on basis of breach as a result of failure to maintain reasonable security

• But implementing and maintaining reasonable security procedures following the breach does not constitute a cure with respect to that breach

• Annual security audits and risk assessments for high-risk companies
  – Subject to rulemaking
REASONABLE SECURITY

• Businesses have a duty to implement and maintain “reasonable” data security
  – In 2016, the CA AG published a report suggesting that compliance with the Center for Internet Security (CIS) Top 20 constitutes a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement these controls arguably constitutes a lack of reasonable security.
    ▪ Controls include: asset inventory, access controls, data and network protection, incident response management and training
REASONABLE SECURITY (CONT.)

- A consumer may bring a civil suit against the business in the event of certain data breaches resulting from the business’s failure to implement reasonable security.
  - Statutory damages of up to $750 per consumer per incident, or actual damages, whichever is greater.
  - Class plaintiffs can be expected to rely on the statutory damages provision, primarily because it supports a large claim for damages and arguably avoids the need to prove any actual harm.
PRACTICAL STEPS TO REVIEW CCPA COMPLIANCE AND PREPARE FOR CPRA
GOALS OF A COMPANY-WIDE CCPA PROJECT

Understand Your Data
- Data mapping and inventory
- Data classification
- Contract review

Implement Compliance Mechanisms
- Policy updates
- Contracting and auditing
- Data security
- Consumer request processing, exception analysis, and technical implementation

Honor Consumer Rights
- Access/know
- Deletion
- Opt-out
- Non-discrimination
- Data portability
PRACTICAL STEPS FOR CPRA PREPARATION

• New consumer rights
  – Evaluate exposure to new advertising “sharing” restrictions
  – Use existing data maps to assess processing of “sensitive personal information”
  – Update consumer request procedures for new correction right

• Update client-facing and vendor contracts with new required contract terms

• Revise information security and data retention policies as needed

• Harmonize privacy notices with new CPRA requirements

• Understand new enforcement agency
  – Evaluate additional obligations for high-risk data processing and profiling
ROADMAP TO 2023

**Near Term**
- Update client-facing contract templates
- Catalog vendors, service providers, partners, and update contracts

**Medium Term**
- Revise privacy notices
- Assess sensitive data processing and exposure to new “sharing” obligations, update data maps

**Longer Term**
- Prepare new consumer request procedures for correction right
- Evaluate changes from CPPA rulemaking
THANK YOU / QUESTIONS

mwe.com