Transatlantic data protection law – a US perspective

GDPR Meets CCPA

Carol Umhoefer

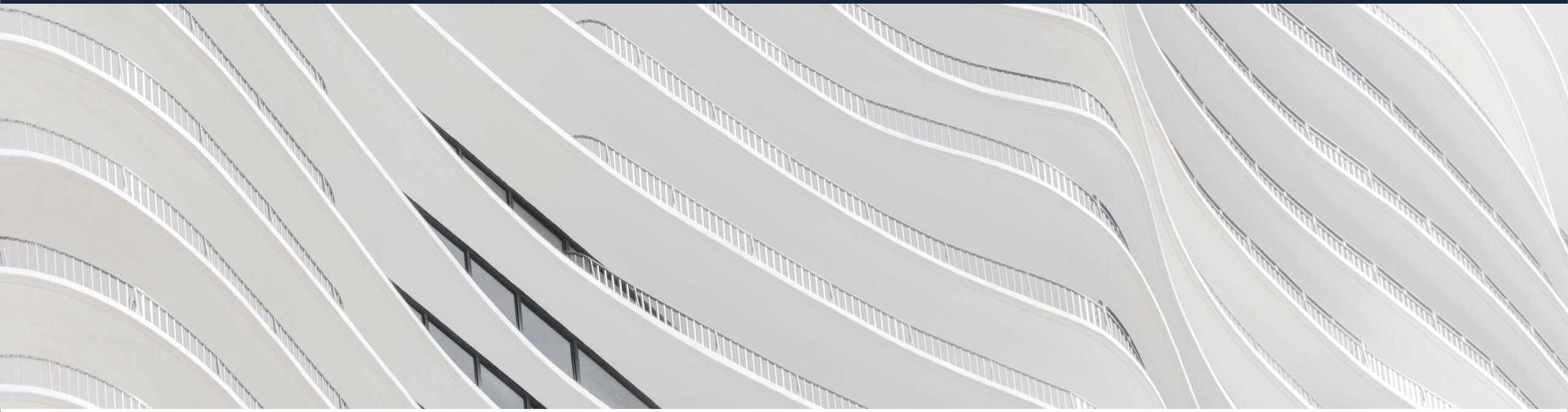
18 November 2020

DLA PIPER

Agenda

1. GDPR's Impact on US Privacy Law & Practice
2. California's Response to GDPR: The CCPA
3. CCPA's Principal Similarities (and Differences) with GDPR
4. Moving the US further toward Europe: The California Privacy Rights and Enforcement Act (CPRA) and Beyond
5. Enter *Schrems II*

1. GDPR’s Impact on US Privacy Law & Practice

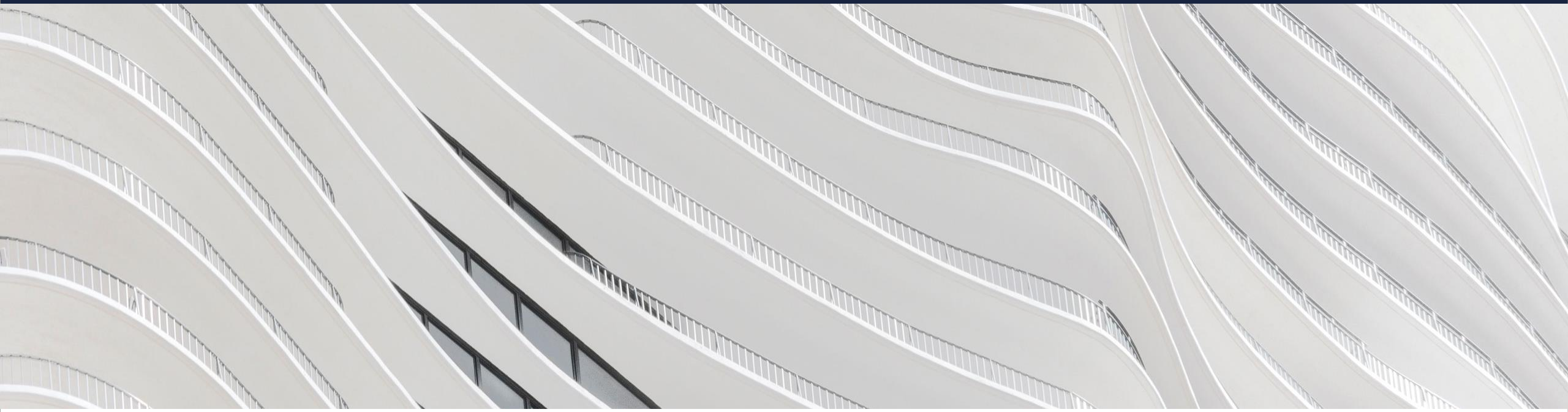


GDPR's Impact on US Privacy Law & Practice

Broad uptake of some aspects of GDPR and European law

- **Greater awareness of privacy and data protection requirements**
- **US-based processors** agreeing to GDPR Art. 28 terms
- **Increased uptake of standard contractual clauses**
- **Recognition that GDPR compliance** eases CCPA compliance for multinationals (data mapping, processes for handling data subject requests, etc.)
- Surprisingly widespread adoption of **cookie banners**
- **Legislative trends** following the EU: Washington State, New Jersey, New York… and California

2. California’s Response to GPDR: The CCPA

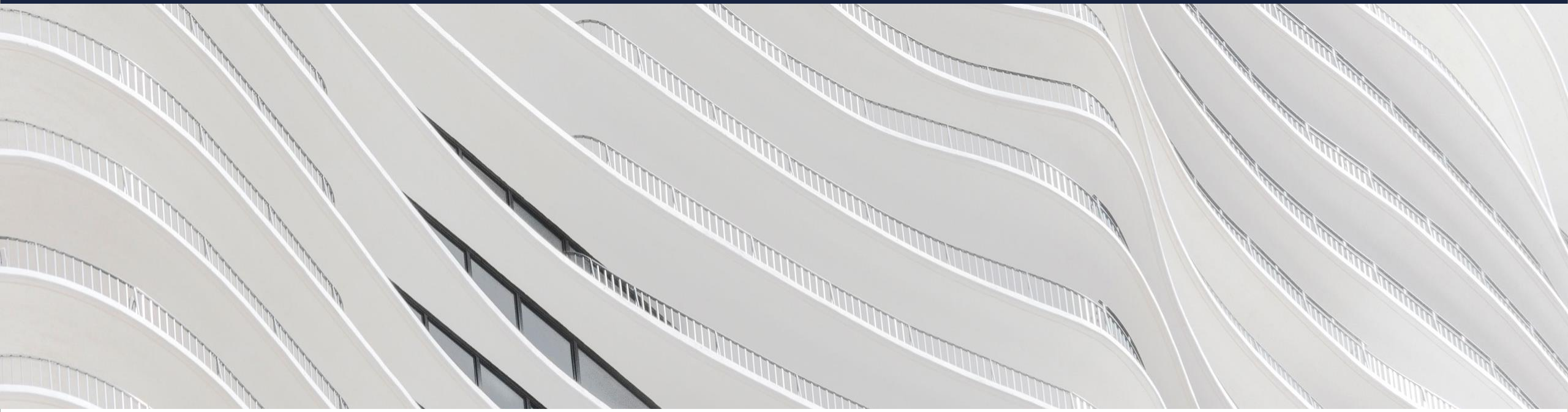


The California Consumer Privacy Act of 2018

California's Response to GDPR

- **California' continues to lead** in US privacy and security law e.g., first in the country to implement a data security breach notification requirement (2001), transparency requirements for list brokering (Shine The Light) (2003); online privacy law (CalOPPA) (2004)
- **First broadly-applicable privacy law** in the US that is not sector specific or limited to specific practices
  - ***Not as comprehensive as GDPR, but broader application than existing laws***
- **Created substantial new rights** for California **residents**, including access rights and portability rights
- **Contains broad definitions** similar to GDPR, such as a broad definition of personal data
- **Took effect January 1, 2020**
  - Privacy provisions enforceable by California Attorney General as from **July 1, 2020**

3. CCPA’s Principal Similarities (and Differences) with GDPR



Similarity – Broad Definitions

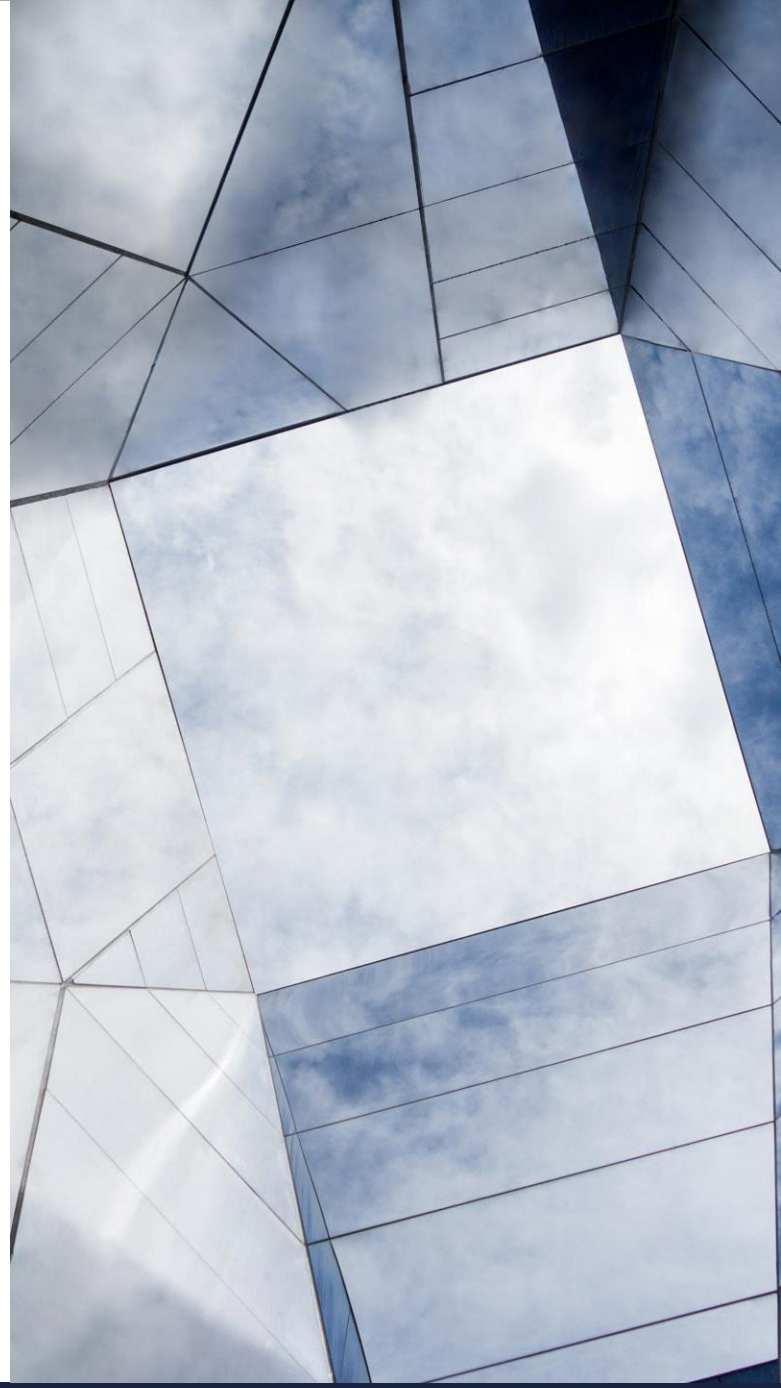
Personal information definition similar to GDPR

- **Personal information: "Any information that directly or indirectly identifies, relates to, describes or can be associated with or reasonably linked to a California resident or household"** — explicitly includes:
  - Name, contact information, government IDs, biometrics, location data, account numbers
  - Employment and education history
  - Purchase history, behavior, and tendencies
  - Online and device IDs
  - Search and browsing history and other online activities
  - Activities from connected devices
- Applies to all California resident personal information - **consumers, employees, B2B contacts**
- Includes **household level** data and **device** data
- **All public record data exempt**

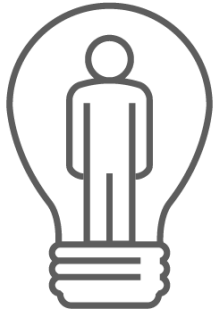
Similarity – Consumer Rights

Consumer rights similar to GDPR

- Right to **know** about how personal information is used, shared and sold
- Right to **deletion** of personal information
- Right to **access** (obtain a copy of) personal information
- Right to **portability** of personal information, if in electronic form
- ***But also:***
- Right against "**discrimination**" for exercising rights
- Right to **sue** for statutory damages for many data breaches



Similarity – Transparency



- **Notice at collection**: Must describe what personal information is collected and why it is used, not later than at the time of collection
- **Privacy policy:**
  - List categories of personal information that is collected, sold, and shared for a business purposes in prior 12 months
  - Specific categories defined in the statute
  - Describe purposes for collection of personal information
  - Describe rights and how to exercise them

Similarity – Service Providers

- **Service providers** must agree to mandatory contract terms for service providers

  (but GDPR terms are not sufficient!)

  - Restrict use of personal information to performing services under contract
  - Prohibit use of personal information outside the direct relationship between service provider and the customer
  - Prohibit service provider from selling the personal information
  - Include a specific CCPA compliance certification that service provider understands the restrictions

➢ *Absent these specific terms, a service provider will be treated as a "third party" and the sharing of personal information with the service provider may be considered a sale, and the sharing must be described in the privacy policy*

Difference – CCPA's Scope of Application

CCPA applies to "businesses"

"Business" means:

(1) Legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

> (A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
>
> (B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.
>
> (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(2) Any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.

Difference – Sales of Personal Information

- Right to **opt-out** of “sale” of personal information
  - Definition of “sale” includes selling, **making available**, providing, or **disclosing** personal information in exchange for any consideration or thing of value
  - Significant impact on the adtech industry
  - Many sales are made via cookies, which allow an adtech company to collect personal information from a website operator’s website
  - Technical challenges in implementing opt-outs
  - Contrasts with the opt-in obligation under the ePrivacy Directive

- Minors <16: Right to **opt-in** to “sale” of personal information

- Websites must display a “Do Not Sell My Personal Information” link if they sell personal information

Difference – Partial Moratoria

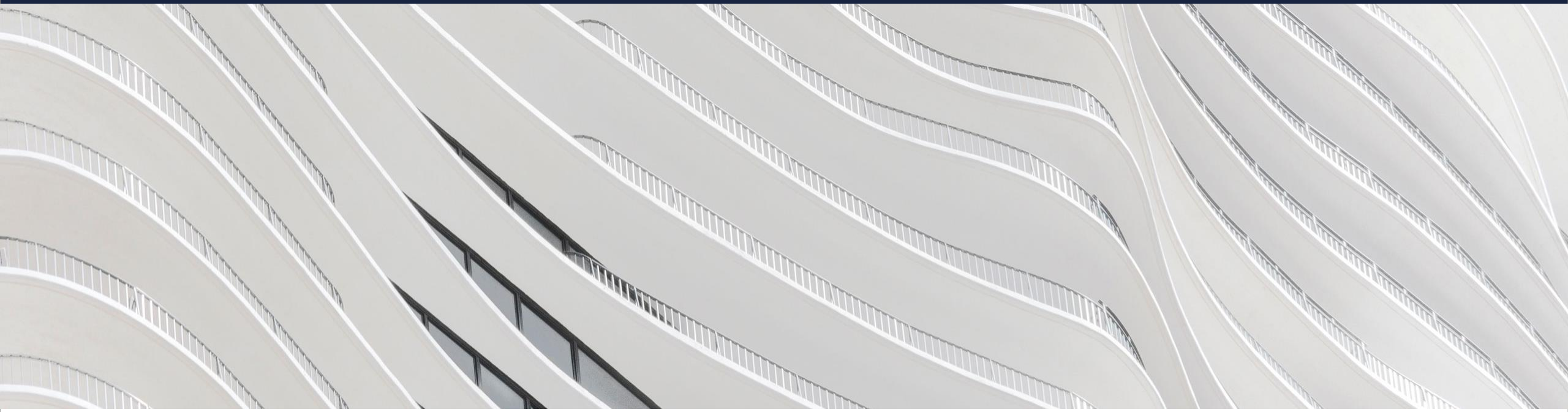
CCPA enforcement delayed until January 1, 2023

- **Business-to-Business Communications**
  - Moratorium applies **only** to information obtained by a business through a communication or transaction with a California resident acting **for another entity**
  - **Does (for example)**
    - delay the obligation to provide notice at or before the point of collection
    - delay the obligations to grant access and deletion rights
  - **Does not**
    - delay application of the opt-out (Do-Not-Sell) or non-discrimination rights
    - apply to information obtained from a third party, such as a list provider
    - apply to B2B communications to prospective customers
    - delay data breach liability
- **Employee Data**
  - Moratorium applies **only** to employee, contractor, job applicant, beneficiary and emergency contact information, provided that the information is collected and used solely in the employment context
  - Delays all obligations **except** notice at time of collection and data breach liability

Difference – Exemptions from CCPA

- **The CCPA does not apply to**:
  - **Medical information** governed by the California Confidentiality of Medical Information Act or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services
  - **A provider of health care** governed by the California Confidentiality of Medical Information Act or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information
  - **Information collected as part of a clinical trial** governed to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration
  - Personal information relating to consumer financial services that is collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act or the California Financial Information Privacy Act (except in cases of data breach liability)
  - Personal information collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994 (except in cases of data breach liability)

4. Moving the US further toward Europe: The California Privacy Rights and Enforcement Act (CPRA) and Beyond



CPRA Aims to Bring CCPA closer to GDRP

Significant New Requirements Starting January 1, 2023

- **Right to cure** eliminated (similar to GDPR)
- **Sensitive data** category created (similar to GDPR)
- New data **minimization** requirement (limited to sensitive data and secondary uses)
- New right of **correction** (similar to GDPR)
- New **service provider obligations** (similar to GDPR)
- **New agency** to enforce the law and engage in rulemaking (similar to EEA supervisory authorities)

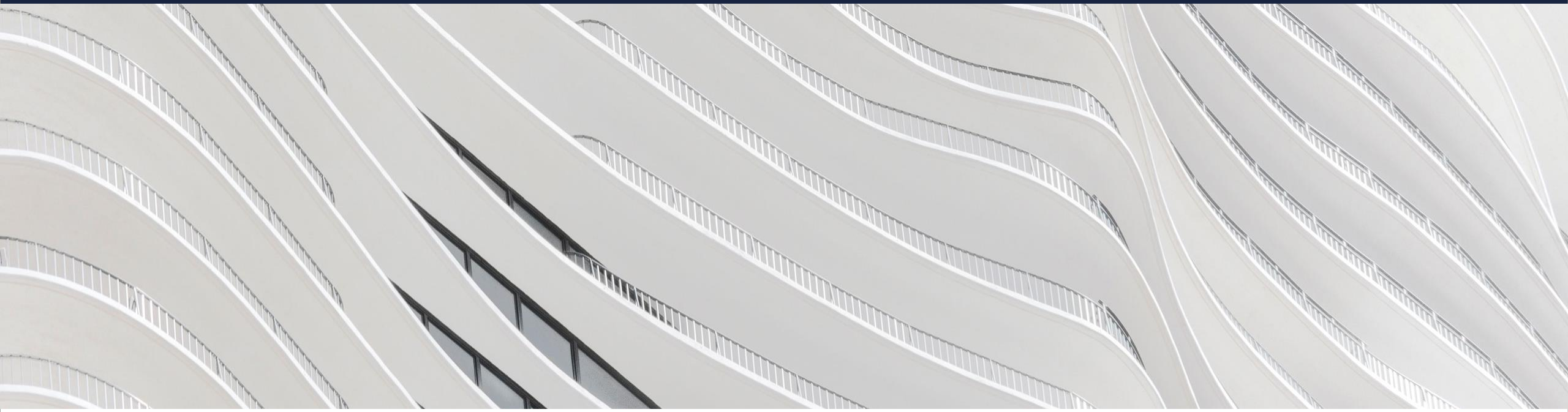
➢ ***But also extends B2B and HR moratoria until January 1, 2023***

Will California Bring the US Closer to Europe?

Legislative Agendas Have Been Hijacked by COVID19

- California's leadership on breach notification laws….
  - … but not on privacy laws
- Initiative in **Washington State** died (twice), may be resurrected
- Other initiatives have stalled (New York, New Jersey…)
- **Federal legislation** may have gotten a boost with Biden election
  - Would federal law pre-empt state law?
    - HIPAA (medical information) did not
    - GLB (consumer financial information) did not
    - CAN-SPAM (email marketing) did

5. Enter Schrems II



Schrems II and the Threat to Transatlantic Data Flows

Will the fall-out push reform in the US?

- ***Schrems II*** could pose existential threats to transatlantic data flows
- **Draft EDPB recommendations** do not appear to reduce the threat
- U.S. government White Paper issued in September 2020:
  - *Most U.S. companies do not deal in data that is of interests to U.S. intelligence agencies*
  - *The U.S. government frequently shares intelligence information with EU member states*
  - *The CJEU did not take all relevant facts into account*

QUESTIONS?

carol.umhoefer@dlapiper.com