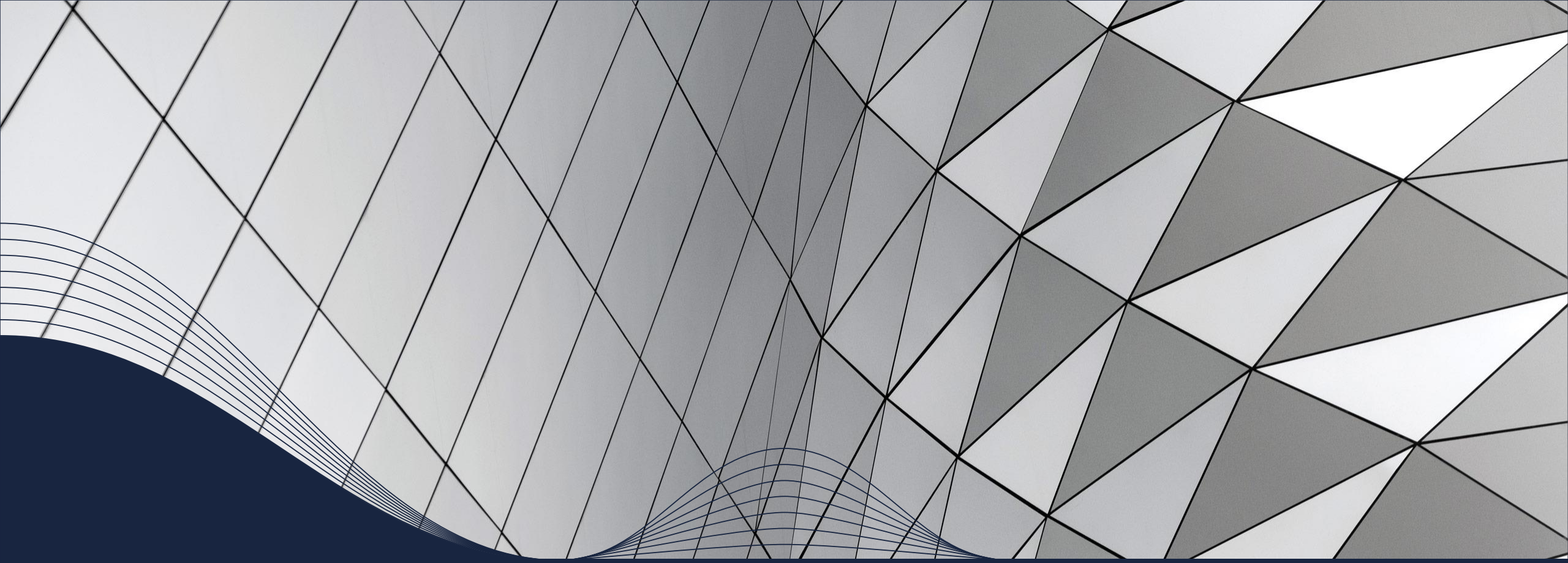
PROGRAM MATERIALS
Program #29128
July 30, 2019

Moving Target: Understanding Coming Changes to the CCPA and Other State CCPA-Like Privacy Laws

Celesq® AttorneysEd Center
www.celesq.com



Emerging US State Privacy Framework vs. GDPR

Jim Halpert
co-Chair Global Privacy & Security Practice
jim.halpert@dlapiper.com

DLA PIPER

**This presentation is offered for informational purposes and should not be construed as legal advice.

California 2020 - CCPA Core Rights

- Transparency ➔ Do Not Sell Button and detailed website notice
- Right to know about disclosures and sales of PI
- Right to opt-out of “sale” of personal information
- Minors <16: Right to opt-in to “sale” of personal information
- Right to deletion of personal information
- Right to access personal information
- Right to portability of personal information, if in electronic form
- Right against “discrimination” for exercising rights
- Right to sue for statutory damages for many data breaches

CCPA Key Likely Amendments

I. **Personal Information**: any information that directly or indirectly identifies, relates to, describes or can reasonably be associated with or linked to a California resident or household

II. **"Consumer" may actually mean consumer!**: Exempt employee, contractor, executive and beneficiary data if collected and used solely in that context (AB 25)

III. **All public record data exempt:** eliminating condition that the information be used for a purpose consistent with the purpose for which the record is made available (AB 874)

IV. **Vehicle recall, warranty and product recall info:** exemptions including for retention and sharing PI between dealers and manufacturers used for that purpose (AB 1146)

V. **Narrow Toll-Free Number obligation for online companies:** if business is exclusively online, may offer only a website and email address to submit consumer requests (AB 1564)

Other State Omnibus Privacy Bills

Nevada (Passed)

- CCPA copycat or similar bills (omnibus rights/opt-in consent bills) failed in CT, HI, IL, LA, MD, NH, NM, NY ND, OR, RI, TX, VA, WA
- Opt-out of Sale of Personal Information Passed in NV (SB 220)
  - Narrower scope of information than CCPA
    - “sell” actually means sell
    - “consumer” means consumer
    - “personal information” applies on to information that is reasonably identifiable
    - GLBA, HIPAA and vehicle service and repair exemptions
  - Builds upon transparency right already in law
  - No PRA for violations of statute

Other State Omnibus Privacy Bills

Washington, Failed in ’19, but Will Be Back

Washington Privacy Act

- Strongly influenced by GDPR
- Clearer Definitions
- Processor/Controller terminology
- Rights of Access, Deletion, Restriction of Processing, Objection to Marketing & Advertising
- Provision Requiring Risk Assessments
- Provision regulating Facial Recognition
- Senate version did not have PRA, House version did.

- Likely to pass in some form in 2020 – sticking points were Private Right of Action, Exceptions, Facial Recognition
- Significantly different model from other omnibus bills.

Other State Omnibus Privacy Bills

Other Omnibus Rights Bills pending in NJ, PR, MA

- NJ – 2 bills (Senate & Assembly) – most like NV
  - Online data only, clearer definitions than CCPA
  - Transparency
  - Right to Know, and
  - Opt-Out of Sale rights
- **Puerto Rico SB 1231** – Omnibus privacy bill likely to change significantly but may move in some form
- **MA SB 120** – Broader than CCPA, has not moved since introduction
- **CT, HI, LA, TX, RI, OR Study Commissions** – all scheduled to meet or continue to meet next year.
  - Some privacy legislation likely in these states

Privacy Impact Assessment (PIA)

GDPR Right Similar to WA Privayc Act

- A PIA mandatory before processing personal data for operations that are likely to present high privacy risks to data subjects due to the nature or scope of the processing operations.
- Authorities listing the type of operations subject to PIA.

Record of processing activity

GDPR Right Not Found in Any US State Law

- Each controller and, where applicable, the controller's representative in Europe, shall maintain a record of processing activities for which it is responsible.
- Also applies to processors in the US who access EU personal data.
- Instead of registering data processing with privacy authority, but simple failure to keep records is a violation that can be sanctioned.

Presenter to read NY Code

This code is required for all attorneys wishing to receive CLE credit in the state of NY

Please notate it carefully

The presenter will only be able to read the code twice and will not be able to repeat it or email it to you.

Thank you!

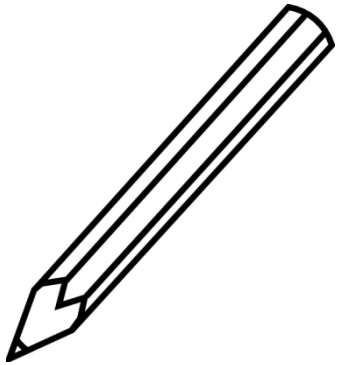
Data Protection Officer

Not Found in Any US State Law

- Obligation applies to controllers and processors.
- Applies when core activities:
  - require regular and systematic **monitoring of data subjects on a large scale**;
  - consist of processing on a large scale **"special categories of data"** (Art. 9) or data relating to **criminal convictions**.
- Who:
  - a **staff member or a consultant** (service contract)
  - Must be **independent**
  - a group may appoint a **single DPO**.

GDPR - Rights of Individuals (May 2018)

New GDPR Rights in Red



- Information (notice) prior to actual data processing
- Right of access
- Right to correct personal data – not in CCPA
- Right to object – in WA Privacy Act
- Right to restriction – in WA Privacy Act
- Right to data portability – in CCPA
- Right to be forgotten vs. 1st Amendment/CCPA exception for “rights of other persons”
- Right not to be subject to automated decision making – not in CCPA

High-level comparison – GDPR and CCPA

Compliance with GDPR is NOT Enough (about 70%)

	GDPR	CCPA
Data definition	• Any information related to an identified or identifiable living natural person	• Broader definition includes information that relates to, or is capable of being associated with, an individual, device, or household
Privacy policy/notices	• More detailed notices, layered approach acceptable, distinction between data collected from individual vs. collected from other sources	• Less detailed notices + prescriptive as to placement of notices and manner in which it must be given
Sale of data	• No absolute right to opt-out of sale, but conditional rights to object to processing • Rights to access with narrow exceptions	• Right to opt-out of disclosure (sale), subject to limited exceptions; entity must display opt-out link on website • Right of access limited to data collection in past 12 months; fewer explicit exemptions

High-level comparison – GDPR and CCPA

Compliance with GDPR is NOT Enough (about 70%)

	GDPR	CCPA
Individual rights	• Conditional rights to erasure, to object to processing and to restrict processing • Right to portability with broader exceptions and narrower range of in-scope data	• Conditional right to erasure, no right to object to processing, no right of restriction or amendment • Right of portability with fewer exceptions and broader range of in-scope data
	• No explicit right against discrimination but discrimination may render processing unlawful	• Right against unreasonable discrimination for exercising rights
Class actions	• No class actions for statutory damages	• Data breach class action for statutory damages
Enforcement	• Antitrust-sized administrative fines (up to 4% global group revenue for serious violations)	• Potentially high California AG enforcement ($7,500 per violation if intentional)

CCPA's Challenges for a GDPR Program

- **Different scope** (includes device, household information; excludes publicly available information; exempts some health, financial data)
- **Different data subject rights**
- GDPR **data mapping** will not be sufficient (sale of data)
- Need CCPA-specific **privacy notices**
- Advisable to amend **business contracts** (cooperation in responding to requests, tracking sales of data, flow down to service providers' processors)
- **Totally different data breach class action risk**
  - Only defenses are name removal encryption or redaction, arbitration clauses
  - No eDiscovery expense in Europe

Sweeping Definitions – Personal Data Conundrum

Companies need to reassess how they think about data

- Must be able to respond to deletion, access, portability, do not “sell” and non-discrimination requirements for this sweeping range of data
  - How to identify, track and act on PI received from different channels that is not identified?
  - Need to identify CA resident data
  - Need to make data more retrievable, strong incentive to create data lakes
  - Need to authenticate requester, including requests by agents
- Must account upon request for types of disclosures and sales of this PI
- Need to notify service providers of data deletion requests

Why It's Hard - Sweeping Definitions

Must Identify and manage personal information that is/may be subject to CCPA:

- ***Consumer*** currently includes any California resident (consumers, B2B contacts, employees)
- ***Personal information*** is "any information that directly or indirectly identifies, relates to, describes or can be associated with or reasonably linked to a California resident or household" – includes information related to individuals, households and devices
- ***De-Identified data exception is almost meaningless*** – circular with this PI definition, except if data are aggregated
- ***Collection*** includes buying, renting, obtaining, gathering, **receiving**, accessing (**actively or passively**) personal information, or deriving personal information from other information, including for profiling
- ***Sale*** includes making available or disclosure of personal information for anything of value in return
- ***Publicly available*** *data* -- Narrow exclusion for publicly available *data* *from government records only and only if for a consistent purpose*
- ***Exceptions*** – What data are governed by CMIA, what are data subject to the GLBA?
- ***MANY drafting errors***

Challenges for GDPR Programs

- **Control processes** designed for GDPR unlikely to be fit for CCPA without amendment
- **Different scope and definitions** (devices, household information, publicly available information, health and financial data)
- **Different data subject rights**
- **Different privacy notices**
- **GDPR data mapping** will **not be sufficient**
- **Commercial agreements** amended for GDPR will need to be further amended (specific terms to avoid qualification as ‘third party’, cooperation in responding to deletion requests)

Great Opportunity for Omnibus Federal Privacy Law

- Long a goal of privacy advocates and some businesses
- Blocked previously because of partisan and committee jurisdiction fights
  - Federal law has been stove-piped, reflecting committee jurisdiction
- Significant interest, serious bipartisan efforts in both the House and the Senate
- CCPA has convinced hold-out businesses to support legislation
- No federal law without:
  - Robust privacy protection
  - Strong federal enforcement, state AG enforcement, no PRA
  - Mechanism to keep up with technological change
  - Broader than CCPA but preempting new state laws

Thank you