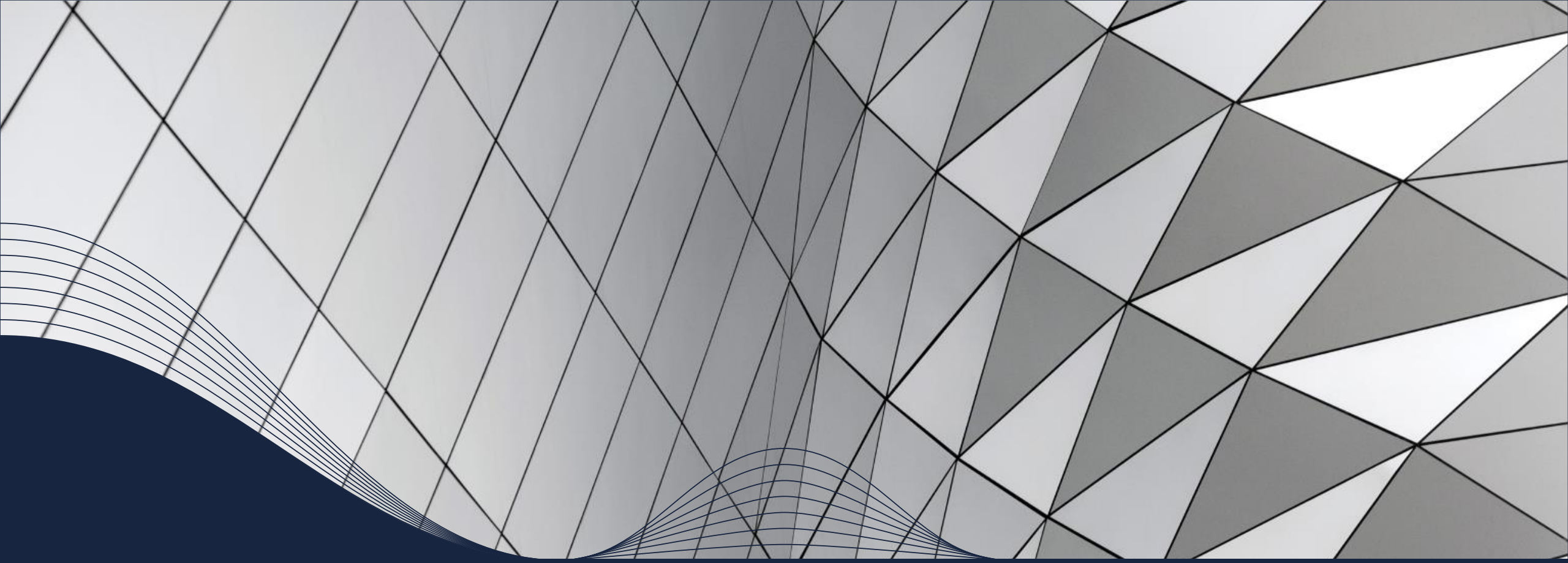


Data Privacy Deep Dive: The California Consumer Privacy Act

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

DLA PIPER

ACC Association of Corporate Counsel CHICAGO

What is the CCPA and why is it a big deal?

- **Game-changing new privacy law** broadly applicable to **businesses** (regardless of location) that collect **personal information** about California residents
- **Substantial new rights** for CA residents
- **Significant operational impacts** for covered business, requires significant time and effort to prepare, but some details of the law will likely change
- **High potential fines** for privacy violations
- Potentially **massive class action liability** for data breaches
- **Broad definitions and scope**
- **Took effect January 1, 2020** (CA Attorney General is to issue implementing regulations by 7/1)
  - Privacy provisions enforceable by CA AG **July 1, 2020**
  - Data breach private right of action available from **January 1, 2020** - **no grace period**

Key Components - Overview

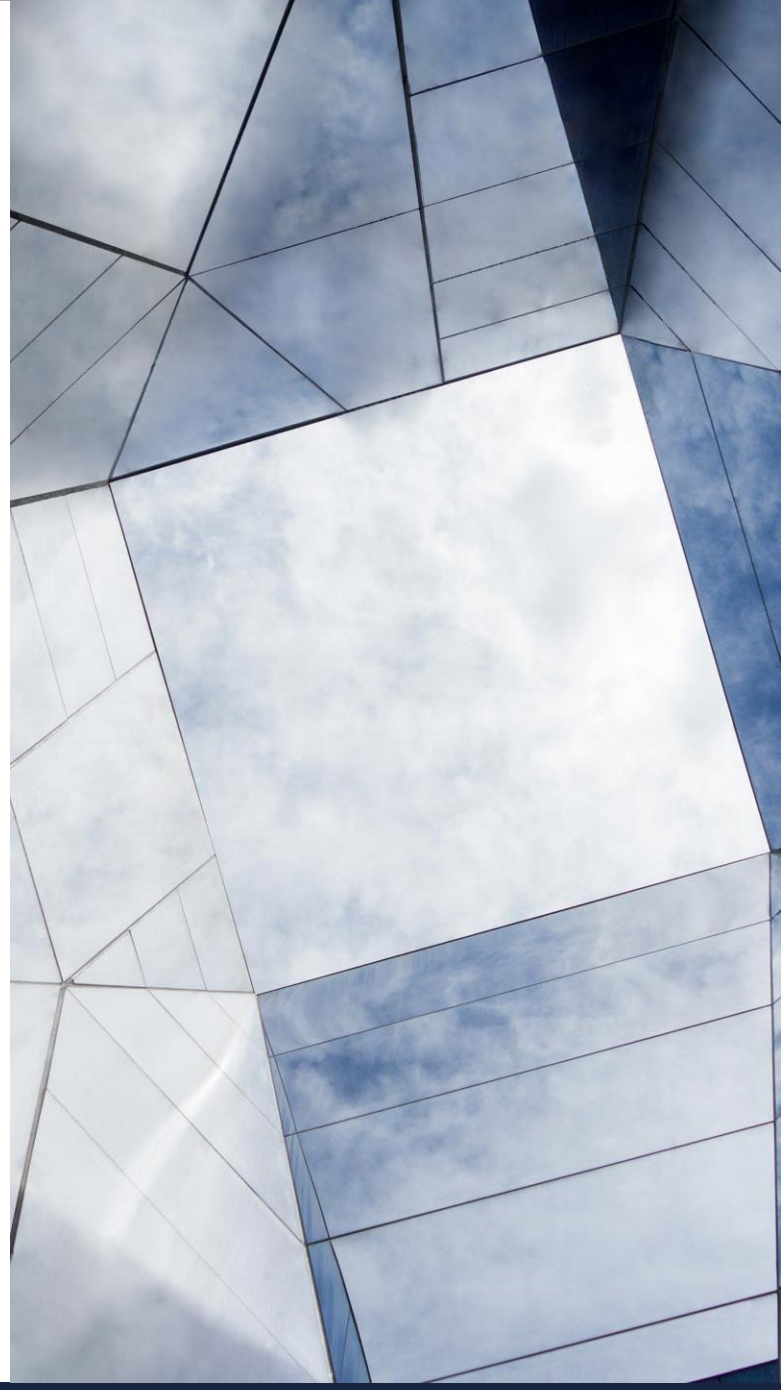
- **New Consumer Rights** (access, deletion, opt-out, information, non-discrimination)
- **New Transparency Requirements**
  - **Notice** of collection and use at or before collection
  - **Privacy policy** requirements
  - **Website updates** and consumer rights mechanisms
- **Vendor and third party management**
  - “Service providers”
  - Third party disclosures
  - Resale of data
- **Private statutory damage right of action** for data breaches regardless of harm

CCPA Scope – covered businesses

- "**Business**" is any entity that **collects personal information** about California residents and **makes decisions** (alone or jointly with others) about how and why the personal information is processed, **if the business either –**
  - (a) has ***annual gross revenues over $25 million*** **OR**
  - (b) annually buys, sells, shares, or ***receives personal information of 50,000+ consumers*****, OR**
  - (c) derives 50% or more of annual revenue from selling personal information
- Also includes parents or subsidiaries (with common branding) of businesses that meet the above
  - But **lateral affiliates are treated as separate companies**
- **Non-profit entities & governments** are not covered
- **Limited exemptions for certain regulated entities**
  - Partial exemption for entities and information covered by certain federal and California health info and financial privacy laws
  - Financial services not exempt from data breach private right of action

California 2020 - CCPA Core Rights

- Transparency ➔ Do Not Sell Button and detailed privacy notice on website
- Right to know about disclosures and sales of personal info (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, with exceptions
- Right to request access to personal information
- Right to portability of personal information, if delivered in electronic form
- Right against unreasonable “discrimination” for exercising rights
- Right to sue for statutory damages for many data breaches



Key Components – New Consumer Rights

Individuals have rights to —

- **Access and obtain copy** of personal info collected in past 12 months
- **Learn how a business has handled the individual's personal information in the preceding 12 months:**
  - Categories of personal info collected
  - Sources of personal information (by category)
  - Purposes of collection, use, disclosure and sale
  - Categories of personal information sold and disclosed
  - Categories of third parties to whom personal info has been sold/disclosed
- **Requests may be made up to 2xs/year, free of charge**

Key Components – New Consumer Rights (cont.)

Individuals have the right to –

- **Request deletion** of all personal information
- Business must direct service providers to delete
- Numerous exceptions:
  - Certain internal uses e.g., complete a transaction requested or reasonably expected by consumer, perform a contract with consumer, use compatible with context in which consumer provided personal information
  - Detect and prevent security incidents and fraud
  - Newspapers (free speech)
  - Compliance with law
  - Using the consumer's information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information

Key Components – New Consumer Rights (cont.)

Individuals have the right to –

- **Opt out of sale** of personal info
  - Home page link to a "**Do Not Sell My Personal Information**" **page**
  - Resellers of data must confirm compliant notice and opt-out provided
- **Opt-in Consent to sale of minor's** personal info (< age 16)

  → **New category not addressed in COPPA**

Complying with requests

- **May not charge** for exercising rights
- Must offer **equal service and price**, even if consumers exercise privacy rights, but can offer **different service or charge different price** if difference is "reasonably related to the value" of the consumer's data
- Must provide, at a minimum, **toll-free number and a website address** (if business maintains a website) so individuals can exercise their rights

Key Components – Enhanced Disclosures

- **Disclosure at or before collection**: must disclose “personal info” collected and its use
  - Prominent hyperlink on home page to this section of privacy policy
- **New privacy policy requirements**:
  - “Do Not Sell My Personal Information” mandatory link to page to website that allows consumer to submit request not to sell his or her data (or household or device data))
  - Describe rights and how to exercise
  - List categories of personal info collected, sold, and disclosed in prior 12 months
  - Describe purposes for collection of personal info

→ **SIGNIFICANT CHANGES TO PRIVACY STATEMENTS**

Key Components – Service Providers

- Mandatory contract terms for service providers
  - Prohibit recipient from selling the personal information
  - Restrict use of personal information to performing services under contract
  - Prohibit use of personal information outside the direct relationship between person and the (disclosing) business
  - Include a specific CCPA compliance certification regarding above
- Absent terms, vendor will be treated as a “third party” for purposes of disclosures and other obligations

  → **CONSIDER SPECIFYING LISTING DE-IDENTIFICATION AS A USE TO ENABLE ANALYTICS**

- Must notify service providers of deletion requests

Heightened Enforcement Risks

Private right of action and statutory damages of USD $100-$750 per consumer per violation for unauthorized access and disclosure of *unencrypted or unredacted* personal information, *if company did not have "reasonable" security*

- AG posts breach notices where > 500 CA residents on its public website
- No requirement to prove harm, very expensive eDiscovery

  → **significant class action risk if have notifiable breach!**

- **Enforcement of privacy and security provisions by California Attorney General with penalties** of up to $2,500 ($7,500 if intentional) per violation

Operational Impacts and Considerations

Know your data

- Identify, inventory, and map data flows at a level sufficient to meet CCPA requirements
- **Key considerations and challenges**
  - Expanded personal info definition (linkable to an individual or household), establishing “household” relationships
  - Data sources and original acquisition channel
  - Identify categories of personal info, recipients, and purposes for both third party disclosures and (separately) third party sales
  - California residency determination

Operational Impacts and Considerations

- **Governance changes**
  - Makes information governance, including of marketing practices, essential
  - Data can no longer be sold or entrusted to 3rd parties without approval and tracking
- **Privacy disclosures**
  - Inventory and update privacy policies, and plan process for rolling out new policies
  - Update or introduce new notices *at or before collection*

Operational Impacts and Considerations (cont.)

Implement opt-out requirements

- Create opt-out mechanism, front and back end
- Post “Do Not Sell My Personal Information” link
- Key Considerations and Challenges
  - Determining validity of consumer request, preparing for 3rd parties to opt consumers out
  - Front end implementation (how does consumer communicate request to the business) +
  - Back end implementation (how does the business communicate and respond to that request throughout the organization/systems).
  - Resolving Opt-out discrepancies across data acquisition channels
  - Resolving conflicting Opt-out requests for household or device data

Operational Impacts and Considerations (cont.)

Vendor and Third Party Management

- Identify, inventory, and gather agreements with the specific third parties with whom the business shares information
- For each, assess whether the business “sells” personal info or “discloses personal information fore a business purpose”
- Review and update service provider agreements

Operational Impacts and Considerations (cont.)

Establish processes and mechanisms for individual rights requests

- Data mapping, processes, and channels for individual requests
  - Determine what data elements are subject to access and deletion requests, and how they will be pulled and provided to individuals
- Train employees
- Key Considerations and Challenges
  - Determining validity of consumer request
  - 12-month look-back
  - “California Data Segregation” strategy challenges
  - Whether can be provided in a portable/useable format

Key Components – Compliance Management

Assess security measures and breach risks

- Map all “breach notice data”
- Seriously consider obtaining agreement to an enforceable class action waiver clause
- Consider “encryption” or redaction defense/exception to notice (if a tree falls in the forest . . .)
- Consider reasonable security defenses (e.g., ISO 27001, NIST, CA AG Guidance on Online Security Controls)
- Review your and your vendors’ cyberinsurance
- Assess and address vendor risk

Implications for M&A

- Provisions specifically targeted at corporate transactions
- Limitations on use of data purchased though transaction; if data (e.g., customer list) is a key asset, potential valuation issue
- Careful attention to diligence for analytics companies – broad definition of “personal information” brings companies into the regulatory fold (i.e., previously, their data collection was not PII such that they did not have protections in place for data)
- Consider Do Not Sell Compliance
  - Draft regs indicate that information collected before do not sell notice is posted will not be able to be sold

Why It's So Hard – Very confusing

- Closed door deal, drafted in 3 weeks, only made public 1 week before passage
  - Insufficiently vetted and proofed!
- 23+ single spaced pages of dense, ambiguous text, hard to understand
- Lots of mistakes –Conflicting paragraphs about the same topic
  - Numerous cross-references to provisions in other subsections of the bill law, requiring leafing back and forth to understand what a provision means
  - Key definitions are unclear, counter-intuitive or don't make sense
- AG's Office has proposed clarifying only some of these ambiguities in 7/2020 draft rules

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** (B2B contacts, employees have partial 1 year moratorium)
  - ***Personal information*** is "any information that directly or indirectly identifies, relates to, describes or can reasonably be associated with or reasonably linked to a California resident, device or household"
  - ***De-Identified data exception is almost meaningless*** – circular with the PI definition, except if data are aggregated or cannot reasonably be associated with a resident (unlike FTC standard)
  - ***Collection*** includes buying, renting, obtaining, gathering, **receiving**, accessing (**actively or passively**) PI, or deriving PI information from other information
  - ***Sale*** includes making available or disclosure of personal information for anything of value in return (not just monetary value)

Why It’s Hard - Sweeping Definitions

- **What is not a sale?**
  - Transfers to service providers if specific contractual obligations are met
  - Transfer directed by the consumer, or the consumer intends to interact with the third party
  - Transfer of personal info as part of a merger, acquisition, etc.
  - Sharing identifier to communicate opt-out status

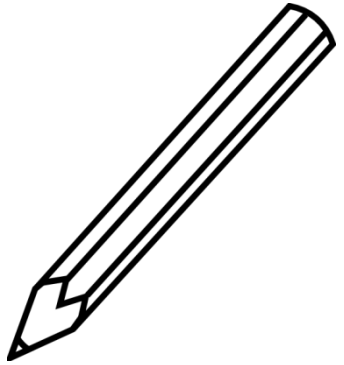
Personal Information Conundrum

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 from a wide range of identifiers
  - Need to make data more retrievable → strong incentive to create data lakes
  - Need to authenticate requester, including requests by agents
  - Need to track do not sell requests
- Must account upon request for types of disclosures and “sales” of “PI”
- Need to notify service providers of data deletion requests

GDPR - Rights of Individuals (May 2018)

- Information (notice) prior to actual data processing
- Right of access
- Right to correct personal data
- Right to object
- Right to restriction
- Right to data portability
- Right to be forgotten vs. 1st Amendment
- Right not to be subject to automated decision making



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 not sufficient**
- **Commercial agreements** amended for GDPR need to be further amended (specific terms to avoid qualification as ‘third party’, cooperation in responding to deletion requests)
- **CCPA keeps changing**

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 No explicit right against discrimination but discrimination may render processing unlawful	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 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)

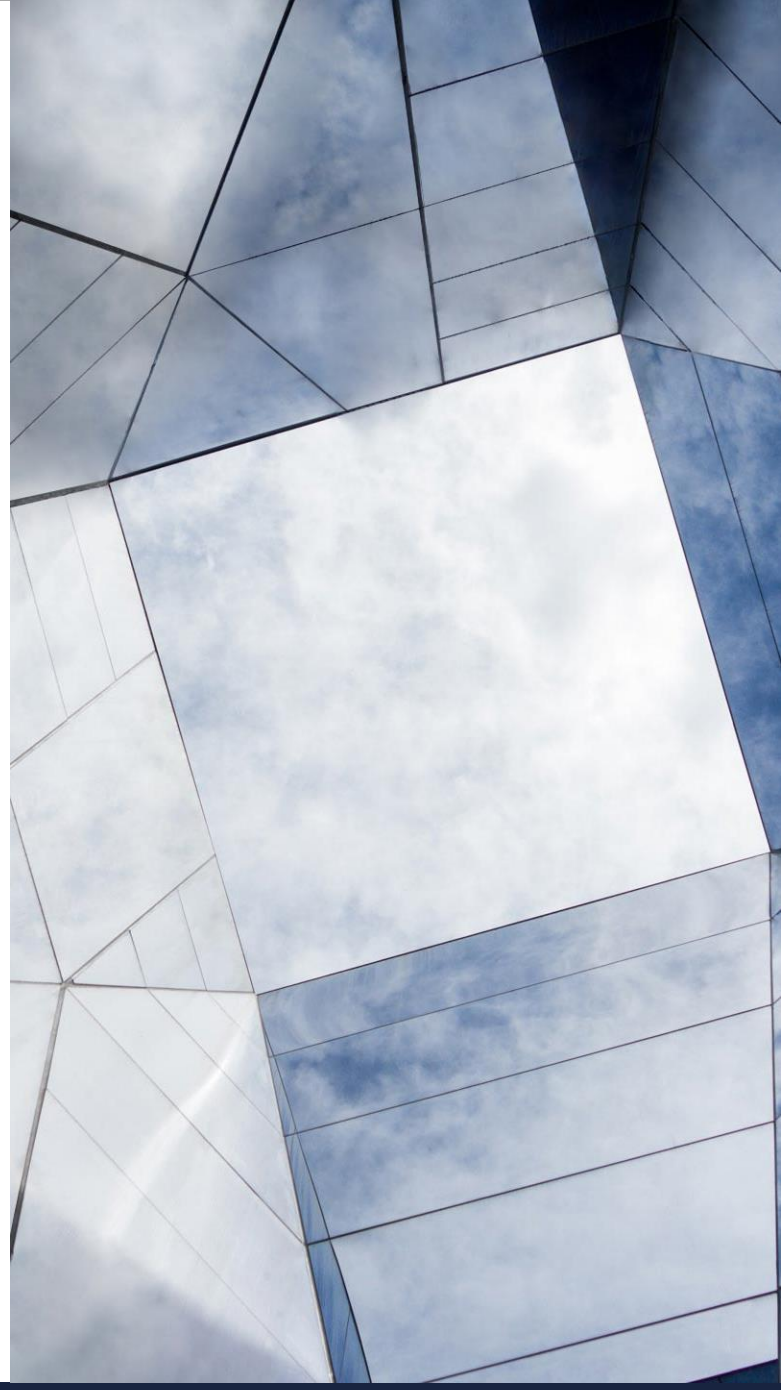
CCPA Key 2019 Amendments

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. **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)

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

IV. **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)

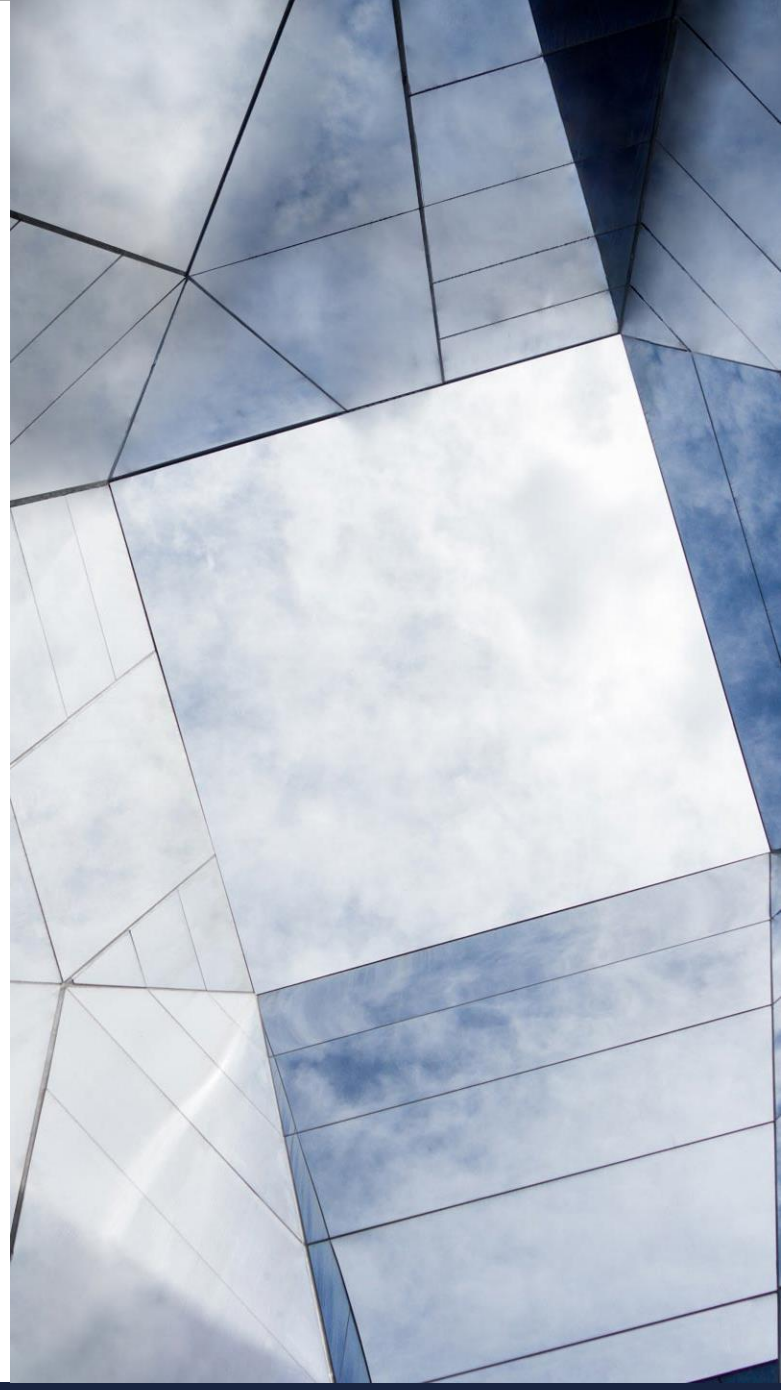


CCPA 2019 Amendments

VI. "Consumer" sort of means consumer for 1 year at least:

- Moratorium for employee, contractor, executive and beneficiary data if collected and used solely in that context (AB 25)
  - Still need to provide short-form notice at or before time of action
  - No exemption from data breach class action risk data

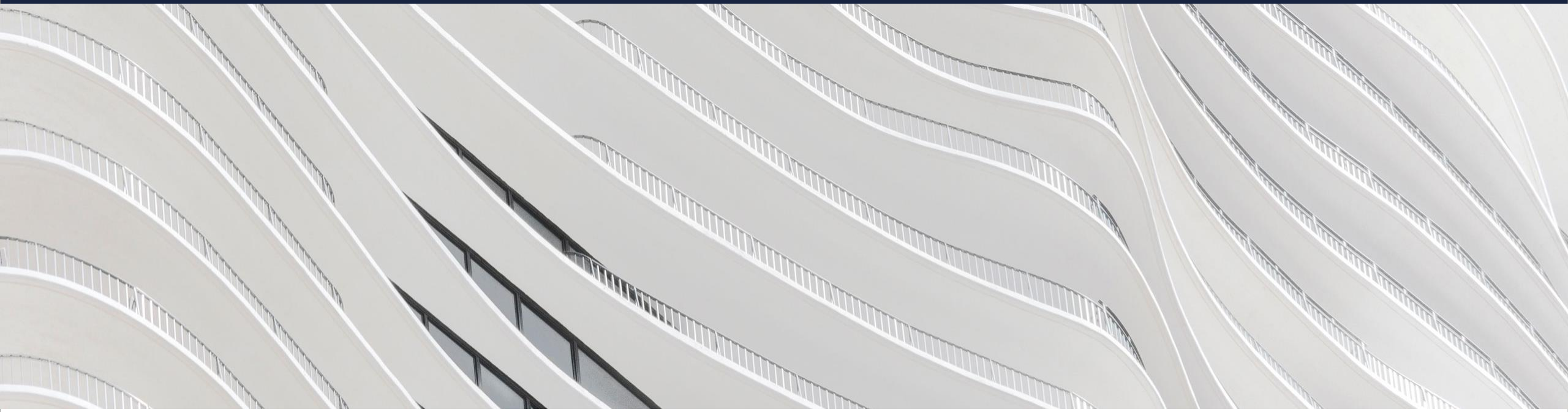
- Information obtained in a transaction with or providing a service to a business, non-profit or government entity
    - Not for Marketing
  - Do Not Sell opt-out right and may not "discriminate" if opt out
  - No exemption from data breach class action risk data
  - But No Notice Obligation



Main Compliance Challenges 1 month In

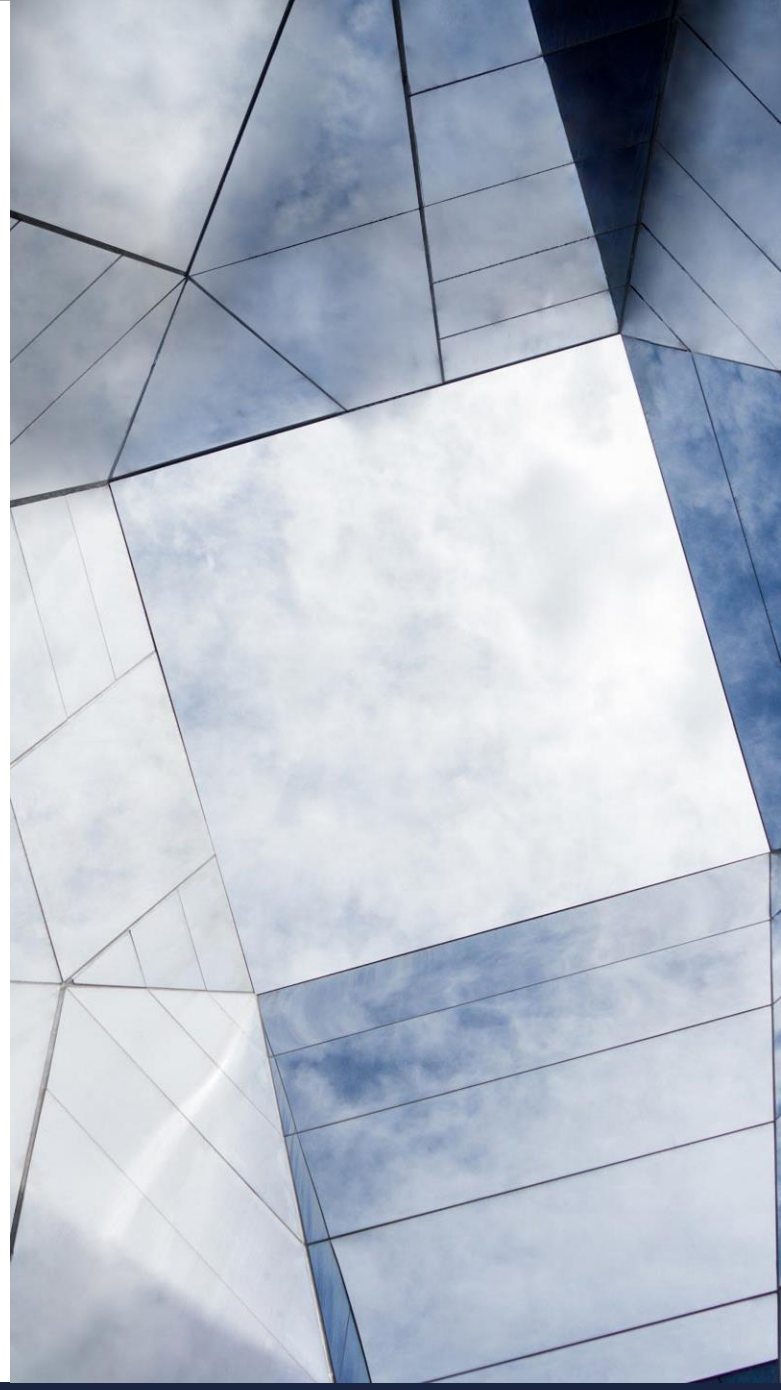
- Data breach risk
  - Only 1 breach notice has been provided to the AG's Office thus far this year . . .
- Selling Personal Information?
  - CCPA definition contemplates allowing behavioral advertising on a site as a sale
  - Google offers restricted disclosure, Facebook moving
  - DAA provides an opt-out icon
  - Privacy advocates complaining about failures to post do not sell
  - Can qualify acknowledgement of a sale
- Vendor management and breach risk ongoing c
- Processing data subject requests
- More changes coming!

CCPA: Moving Target



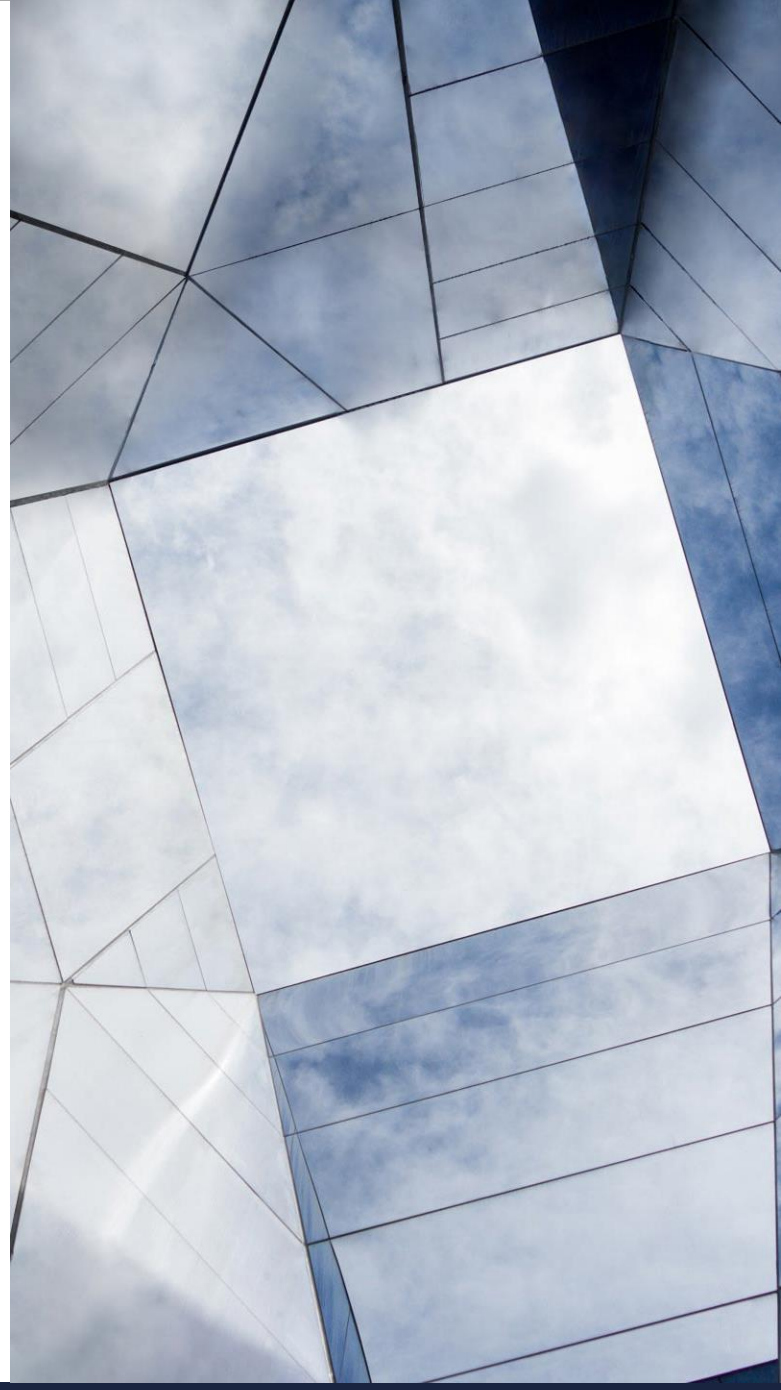
What's Next? - CCPA Rulemaking

- AG Required to Issue Rules Clarifying Several Points in the Law by July 2020
  - What is verified consent?
  - Do Not Sell button and notices, including for incentives
  - Process for submitting and complying with consumer requests
  - Potential expansion of Personal Information
  - Federal law exemptions – trade secrets, IP
  - Rules for consumer authorization of 3rd party agents



Amendments and Rules Will Not Fix

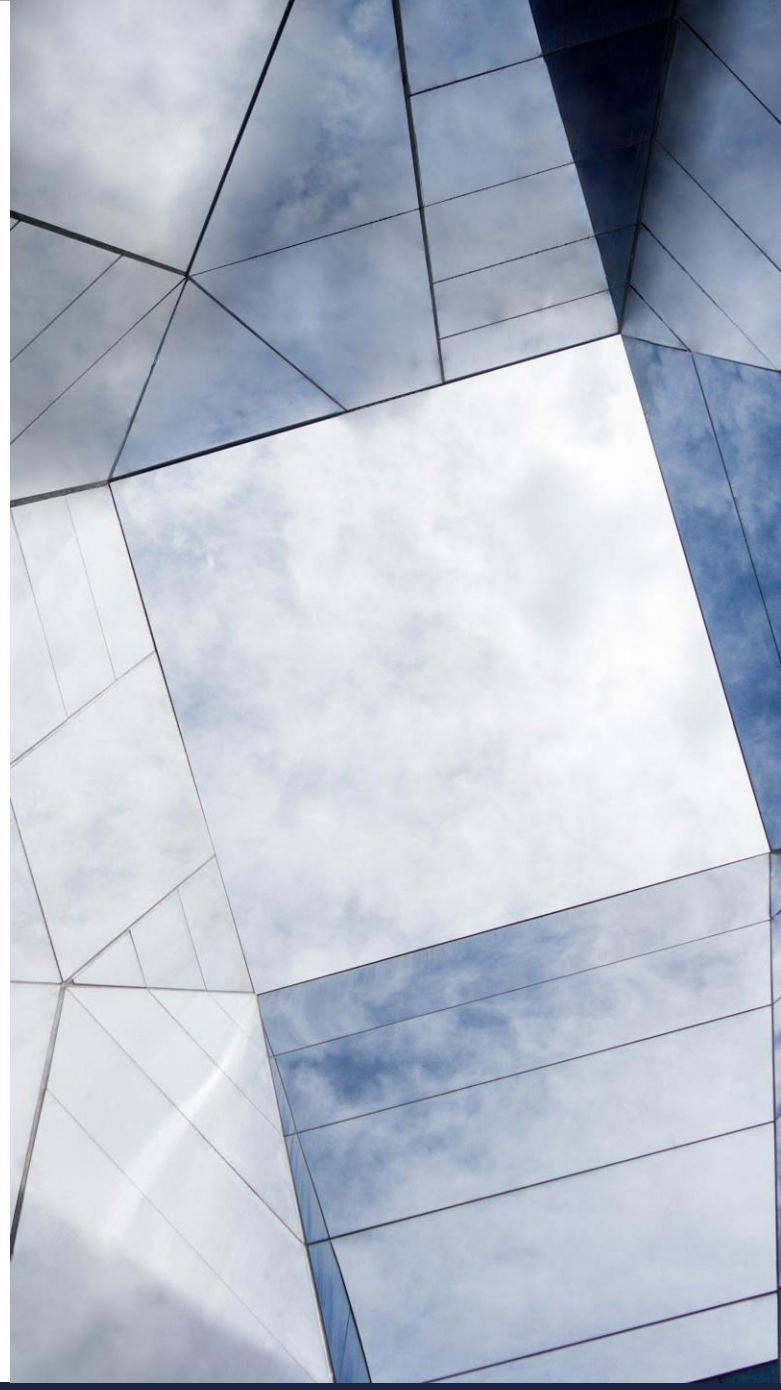
- Many of the confusing definitions
  - Senate Judiciary Committee blocked clarification of de-identified data
    - Incentive to make all data retrievable in order to comply with requests remains
  - Privacy groups and unions limited employee data exemption to 1 year
  - Senate Judiciary Committee killed bill to prevent fraudsters and hackers from opting out of sale of their data for fraud and hacking prevention
  - Exemption to data deletion for research is limited to non-commercial research



2020 Draft Regulations

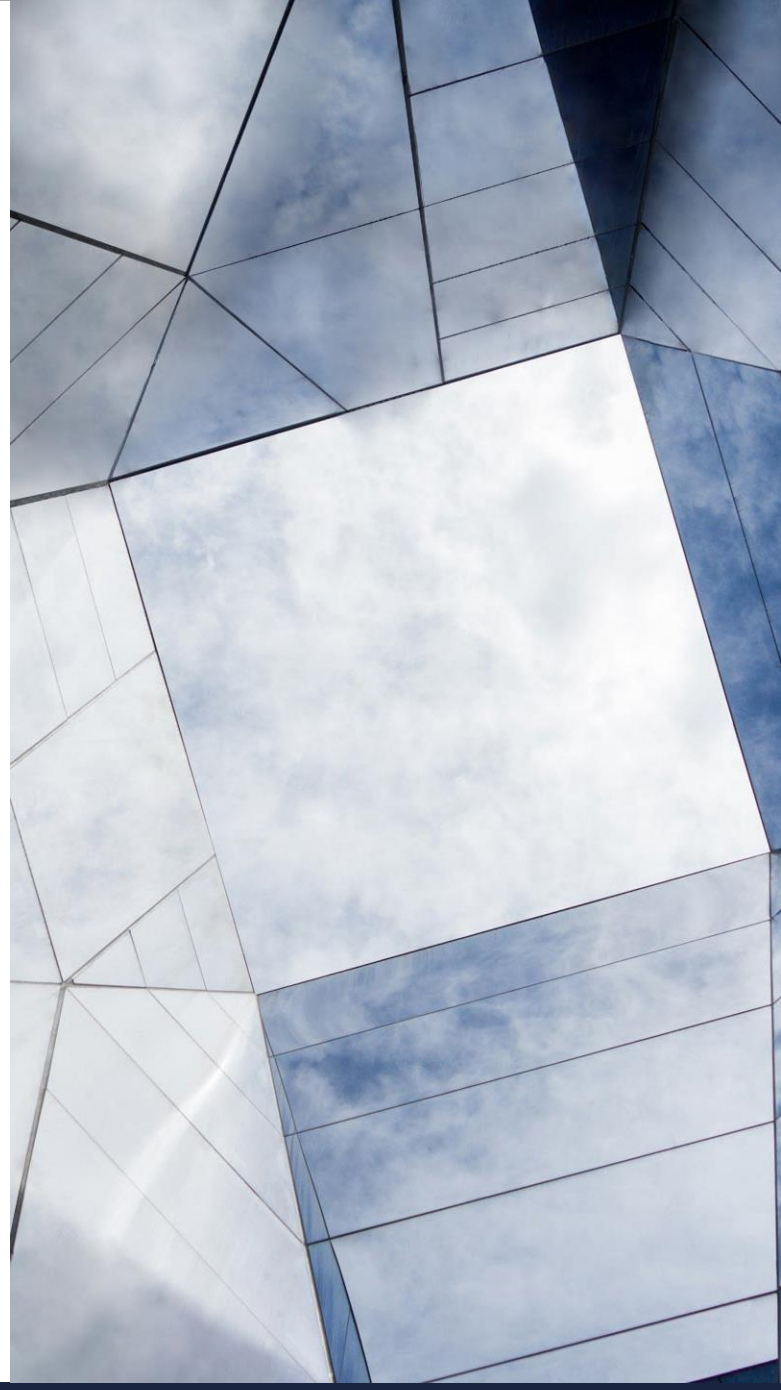
- Will be finalized Q2 2020 and take effect 7/1/20
  - Rumor AG will issue second round of draft regs for comment
- Round 1: New Requirements Going Far Beyond CCPA's Text
  - Much more granular notice requirements, including uses of different data types
    - Opt-in Consent if leave out uses
    - Blanket Do Not Sell Requests must be accepted via browser and other technical settings

      → Mini-Do Not Track
  - Highly prescriptive authentication requirements for access and deletion requests
    - 2-step confirmation of deletion and opt-in requests
    - Potential liability if do not use reasonable verification



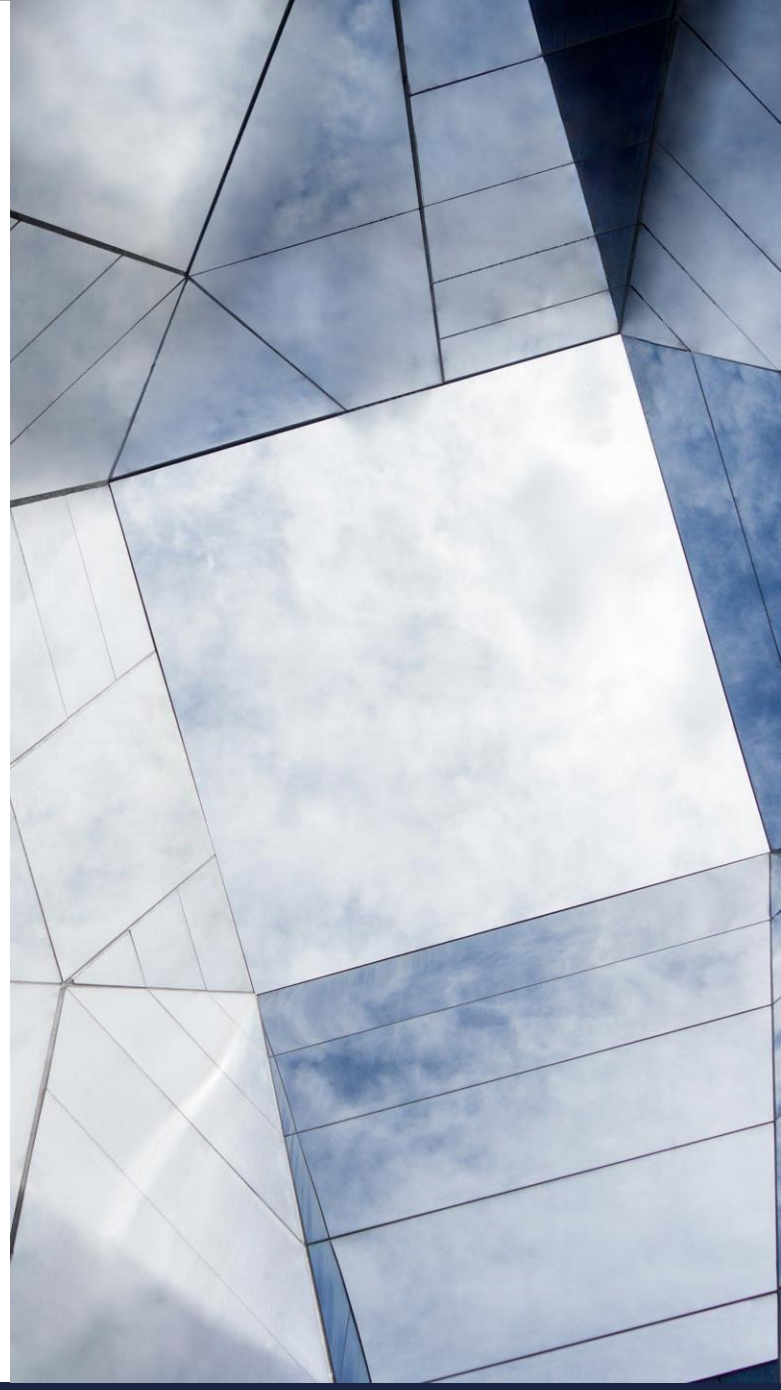
2020 Regulations

- New Requirements Going Far Beyond CCPA's Text
  - May not "resell" personal information obtained from 3rd parties unless obtain a signed attestation from the data source that the CA resident was shown a CCPA compliant privacy notice.
  - Extensive notice and data valuation requirements for incentive programs for consumers to waive rights
  - Data collectors of > 4 million CA residents must publish metrics on response to each type of request
- AG has stated will enforce for violations of clear requirements starting 1/1/20 before regs are final! (requirements in the statute)



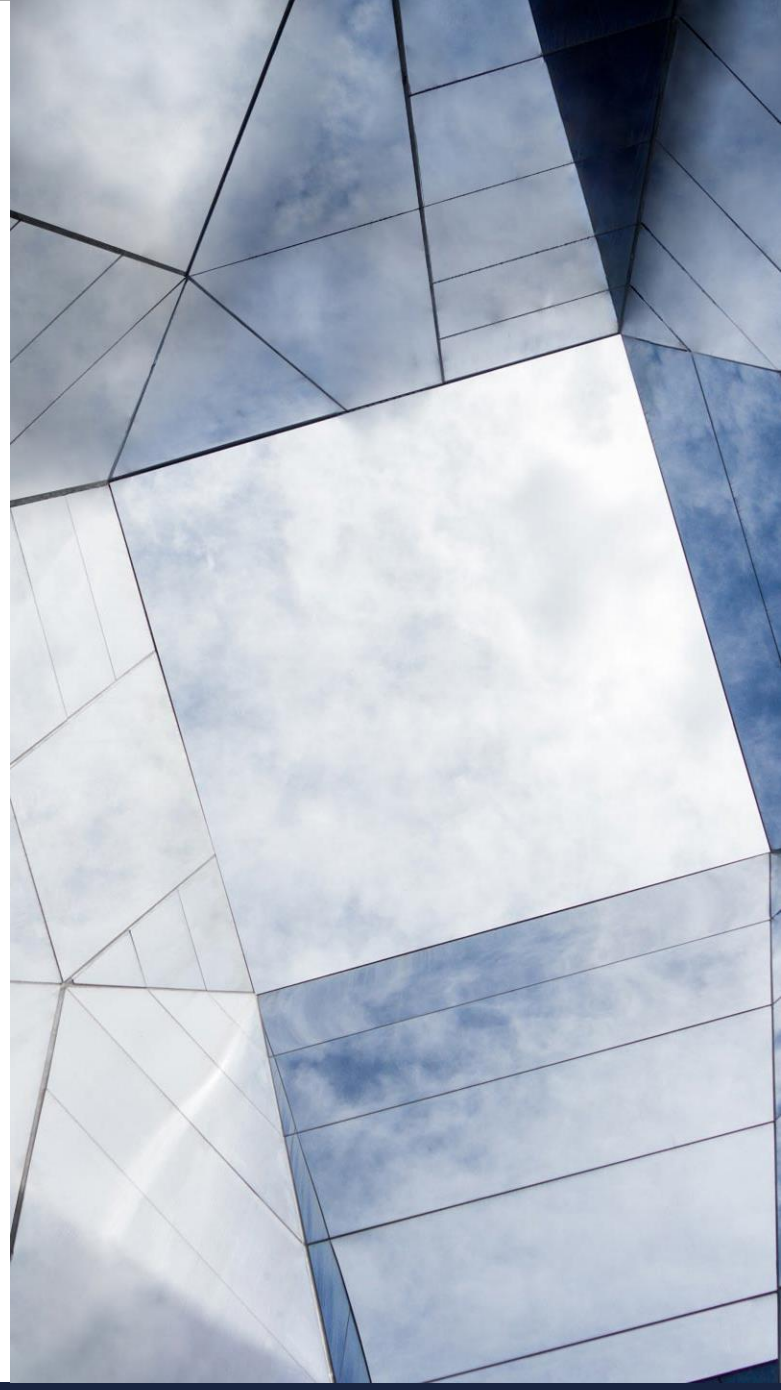
2020 Draft Regulations

- Some Helpful Clarifications
  - No mandatory Do Not Sell icon button (for now)
    - Clear and conspicuous link would suffice
  - May aggregate responses for household data
  - Service providers to gov’ts/non-profits need not respond
  - Exempt sensitive data from disclosure in response to access requests



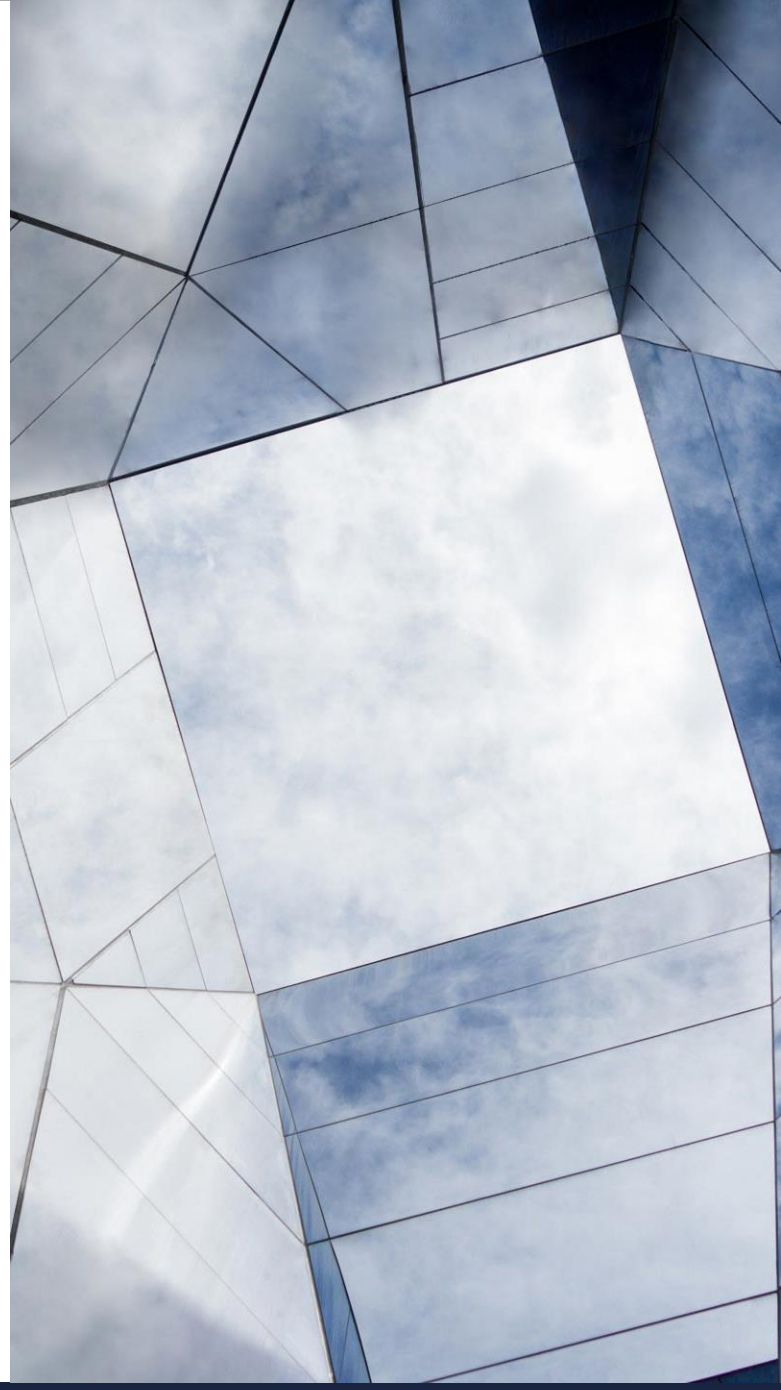
2020 CPRA Initiative

- Filed with Attorney General's Office for Nov. 2020 Ballot -- If approved, would take effect Jan.1, 2023
- Some Operationally Helpful Elements
  - 2 year extension to 2023 of employee and B2B moratoria
  - Data sharing arrangements that are not "sales", now called "sharing" instead of "sale"
  - Unstructured data exception for deletion and access rights
  - Somewhat greater flexibility for non-cross site ad services, and ad metrics
  - Exempts publicly available data
  - Broader security exception, including physical safety



2020 CPRA Initiative – New Requirements

- Right to correct personal information that is inaccurate
- Opt-out of both uses and disclosure of sensitive data, including location data, that are not necessary for the service provided
- Do Not Sell automatic signal is an alternative to Do Not Sell website icon (not mandated), signal is a presumption -- consumer may be asked at websites if he or she agrees to sale
- Limits on retention of personal data to disclosed purposes
- Data breach class action risk for email account credentials
- Removes 12 month look-back limit on right to know and data access requests



Other State Omnibus Privacy Bills

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 restricting Facial Recognition
- Senate version does not have PRA, House version did.

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

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
- But deal will take several years
- Likely outlines
  - Robust privacy protection
  - Strong federal enforcement, state AG enforcement, no PRA?
  - Rulemaking mechanism to keep up with technological change
  - Broader than CCPA but preempting new state laws

In Depth Webinars on specific CCPA issues:

https://www.dlapiper.com/en/us/focus/ccpa-events/.