Emerging US State Privacy Framework

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

**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 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 “discrimination” for exercising rights
§ Right to sue for statutory damages for many data breaches
Why It’s 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 – More than 50 drafting errors:
  - Conflicting paragraphs about the same topic
  - Numerous cross-references to provisions in other subsections of the law, requiring leafing back and forth to understand what a provision means
  - At least 5 cross-references are to the wrong provision!, and
  - Key definitions are unclear, counter-intuitive or don’t make sense
- AG’s Office has indicated that it will not clarify these ambiguities or rules
- 2019 amendments not done until Sept, T-4 months to effectively implement
Why It’s Hard - Sweeping Definition

- Must identify and manage personal information that is/may be subject to CCPA.
- **Consumer** currently includes any California resident (consumers, B2B customers).
- **Personal information** is “any information that directly or indirectly identifies, describes or can be associated with or reasonably linked to a California resident household” – Almost meaningless.
- **De-Identified data exception is almost meaningless** – circular with the definition of data. If data are aggregated or cannot reasonably be associated with a resident (reasonable standard).
- **Collection** includes buying, renting, obtaining, gathering, receiving, accepting (passively) PI, or deriving PI information from other information.
- **Sale** includes making available or disclosure of personal information for a monetary return (not just monetary value).
- **Publicly available data** -- Narrow exclusion for publicly available data from records only and only if for a consistent purpose.
Personal Information Conundrum, Companies need to reassess how they think about data

Ø Must be able to respond to deletion, access, portability, do not sell, and discrimination requirements for this sweeping range of data
  • How to identify, track and act on PI received from different contexts—known or not identified?
  • Need to identify CA resident data from a wide range of identifiers
  • Need to make data more retrievable — strong incentive to consider this
  • Need to authenticate requester, including requests by agents
  • Need to track do not sell requests
Ø Must account upon request for types of disclosures and “sales” of PI
Ø Need to notify service providers of data deletion requests
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)
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 blocked exemption for B2B data
  - 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
Political Stalemate on Fixes

• Privacy Groups
  • All non-profits are exempt, so they are unaffected
  • Harder line groups want significant expansion
  • They objected to fixes on the ground that the law was not being expanded, just clarified in narrowing ways
  • Their ally, Senate Judiciary Committee chair blocked most clarifications, calling the CCPA “weak”

• AG’s Office
  • 1 year after passage, has proposed no clarifications, just proposals to remove burdens on the office

• Business Community
  • So many operational problems, no guidance
  • Technical fixes are lower priority
Other State Omnibus Privacy Bills

- 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
  - Builds upon transparency right already in law
  - No PRA for violations of statute

- Other Omnibus Rights Bills pending in NJ, PR, MA
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 regulating Facial Recognition
- Senate version did 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.
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
Other State Omnibus Privacy Bills

- 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

- **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
2019 – No Private Right of Action

- CCPA has private right of action for some data breaches, Not for privacy violations
  - Core part of CCPA legislative compromise
  - Rights are operationally complex (e.g. locating every IP address)
  - Private lawsuits much more likely to target technical non-compliance that is easy to prove or expensive to disprove

- Two bills in CA, IL and WA Private Right of Action omnibus privacy bills all failed
- NV SB 220 passed after PRA was removed
# High-level comparison – GDPR and CCPA

**Compliance with GDPR is NOT Enough (about 70%)**

**GDPR**

<table>
<thead>
<tr>
<th>Data definition</th>
<th>Any information related to an identified or identifiable living natural person</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy policy/notices</td>
<td>More detailed notices, layered approach acceptable, distinction between data collected from individual vs. collected from other sources</td>
</tr>
<tr>
<td>Sale of data</td>
<td>No absolute right to opt-out of sale, but conditional rights to object to processing</td>
</tr>
<tr>
<td></td>
<td>Rights to access with narrow exceptions</td>
</tr>
</tbody>
</table>

**CCPA**

- Broader definition of information includes any information capable of being associated with an individual
- Less detailed prescriptive requirements for notices and must be given
- Right to opt-out of sale, subject to exceptions; opt-out link on site
- Right of access to consumer's information for explicit exercise of rights
High-level comparison – GDPR and CCPA

Compliance with GDPR is NOT Enough (about 70%)

**GDPR**

**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

**Class actions**
- No class actions for statutory damages

**Enforcement**
- Antitrust-sized administrative fines (up to 4% global group revenue for serious violations)

**CCPA**

- Conditional right to object to processing and right of restriction
- Right of portability with broader exceptions and narrower range of in-scope data
- Right against unfair discrimination including penalization
- Data breach class action
- Potentially higher administrative enforcement ($100 per violation or $750 per intentional violation)
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** (cooperating, responding to requests, tracking sales of data, flow to service providers’ processors)
- **Totally Different data breach class action risk**
  - Only defenses are name removal encryption or re-arbitration clauses
  - No eDiscovery expense in Europe
Challenges for GDPR Programs

- **Control processes** designed for GDPR unlikely to be fit for GDPR amendment
- **Different scope and definitions** (devices, household information, 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 reviewed (specific terms to avoid qualification as ‘third party’, cooperation, 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 preemption
  - Mechanism to keep up with technological change
  - Broader than CCPA but preemption of new state laws