Why *Everyone* Should Care About CCPA

Michele Cohen, Miles & Stockbridge, P.C.
Mid-Atlantic CIO Forum
November 21, 2019

MILES & STOCKBRIDGE

Effective January 1, 2020

The California Consumer Privacy Act is intended to provide a broad privacy protection framework against the unauthorized sale or other disclosure of Personal Information of California residents.

Effective Date: January 1, 2020

Compliance Date: April 2020

Look back provision: January 1, 2019

Implementing Regulations: NOW

MILES & STOCKBRIDGE

Who is covered?

What is covered?

MILES & STOCKBRIDGE

Who Is Covered?

Consumers: CCPA covers all individual consumers residing in California

a. Temporary partial exclusion for employees of Businesses

Business: Entities who collect PI of CA residents, control the purpose and means of processing the PI, and who do business in CA.

Service Providers: Entities who process PI for Businesses.

Third Parties: Persons/Entities other than Businesses and Service Providers buying or otherwise receiving PI covered by CCPA.

MILES & STOCKBRIDGE

Limited Business Control over Others

MILES & STOCKBRIDGE

The Business is not responsible for its Service Providers (generally) or for Third Parties.

But, what does this really mean?

MILES & STOCKBRIDGE

What Is Covered?

Personal Information: Any information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked to, directly or indirectly, with a particular consumer or household.

Clarifications From the Legislative Session

1. De-identified and aggregated information is excluded.

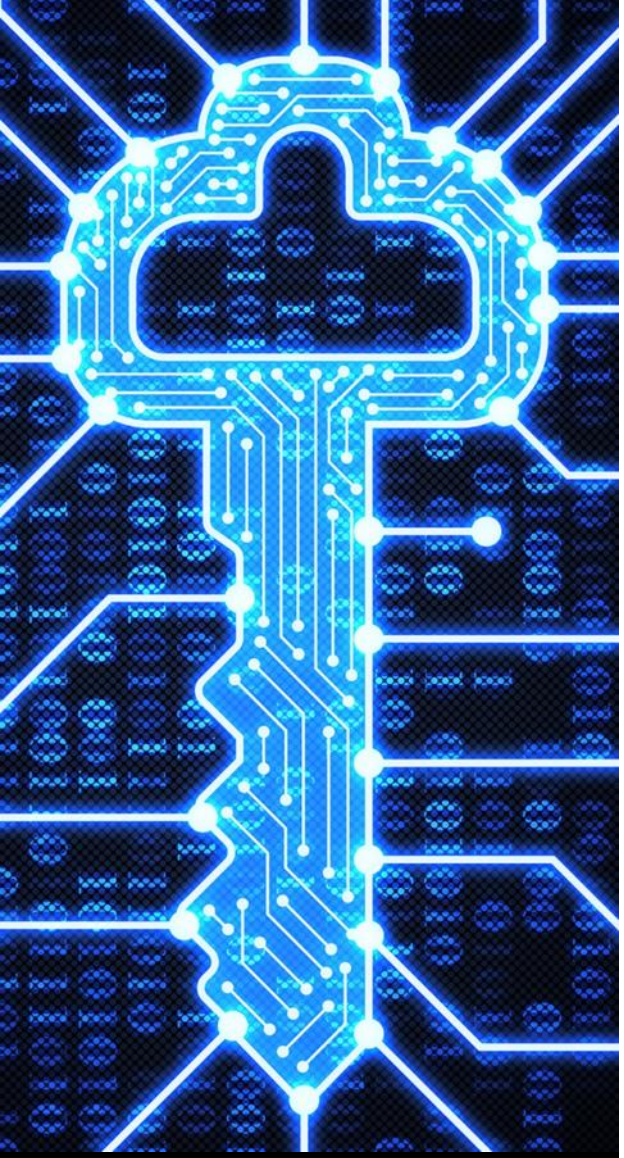
2. Efforts to narrow certain definitions did not succeed in the 2019 legislative session.

3. Expect failed amendments to be introduced in future sessions.

MILES & STOCKBRIDGE

Consumer Rights under CCPA

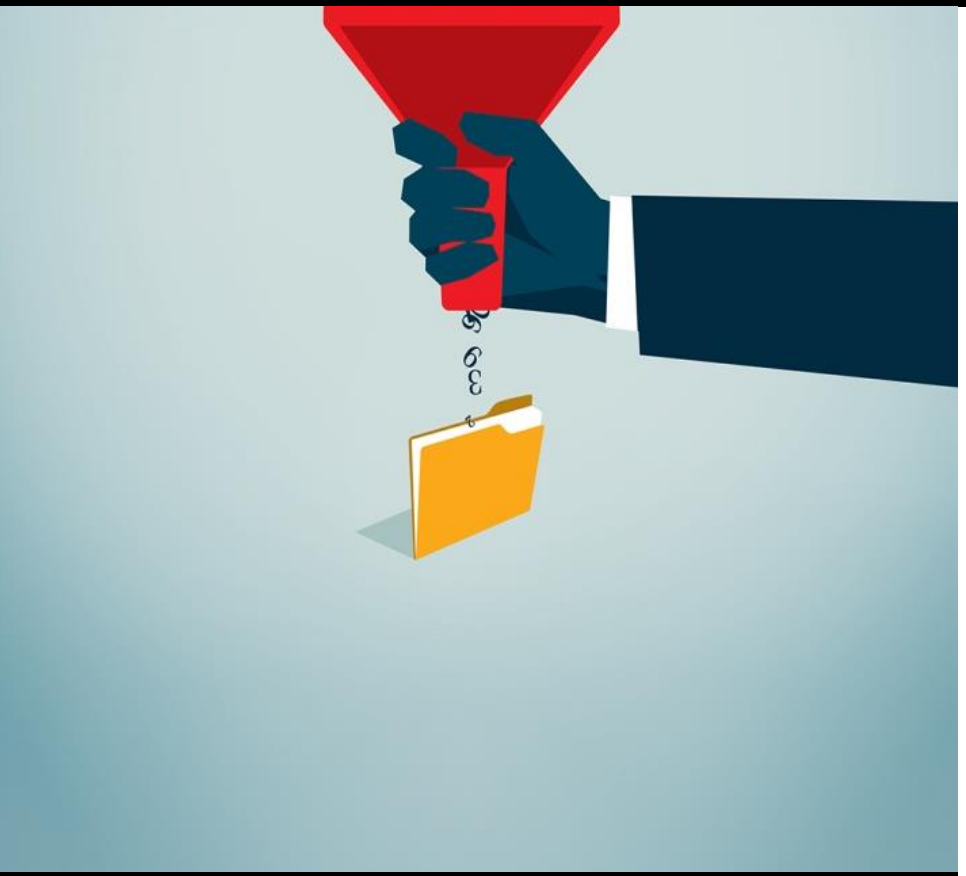
MILES & STOCKBRIDGE



MILES & STOCKBRIDGE

Rights are Triggered when a Business Collects, Sells, Discloses PI

1. Consumers may request details on:
    a. Categories of PI collected and sold
    b. Specific PI collected
    c. Sources from which PI is collected
    d. The purpose of collection
    e. The categories of Third Parties with whom PI is shared (specific as to each category)
    f. The categories of PI disclosed for each business purpose



MILES & STOCKBRIDGE

2. Business must verify the identity of the requestor and the request.

   a. Business may not charge

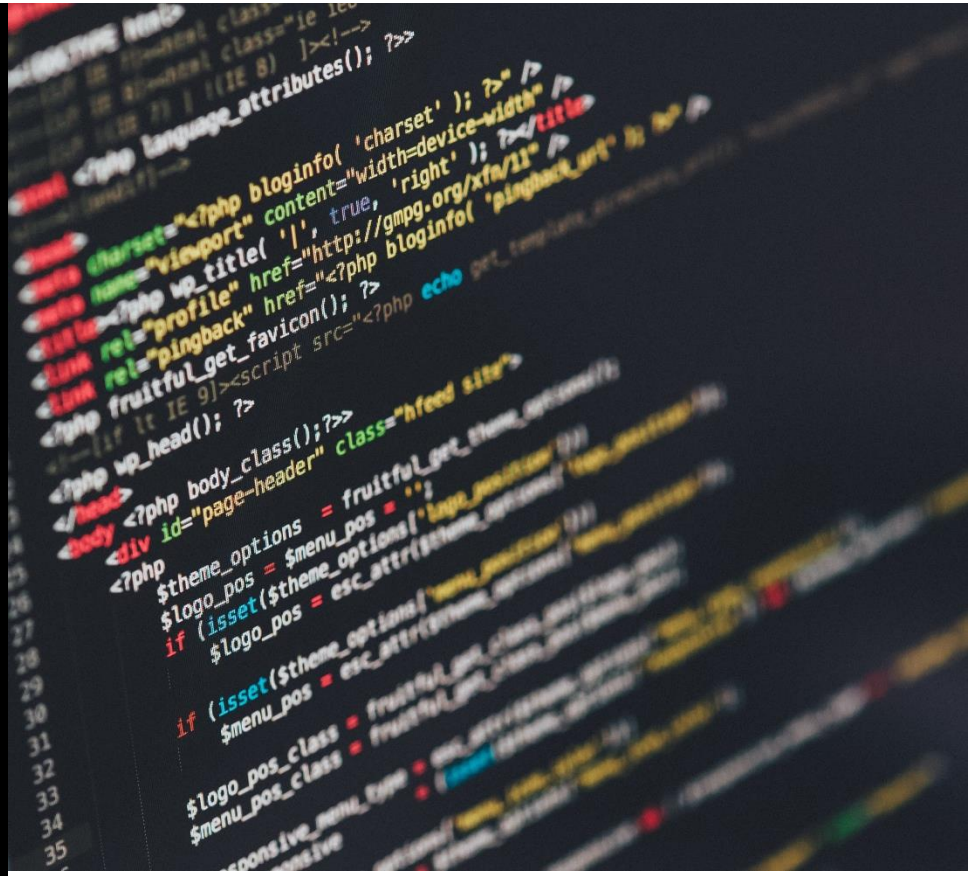
   b. Delivery may be electronic if the transmission is in usable form for further transfer

   c. There are exceptions

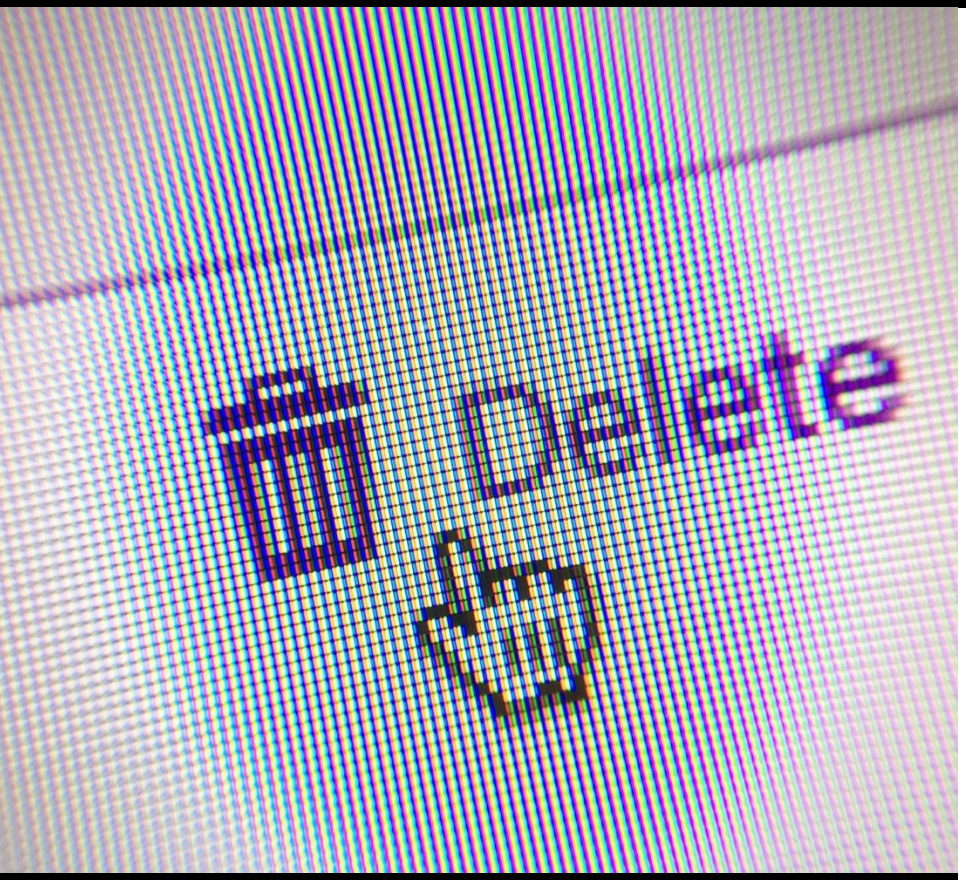
3. Opt-Out Rights

a. Consumers may opt-out of having their PI shared/sold

b. Special rules for minors



MILES & STOCKBRIDGE



MILES & STOCKBRIDGE

4. Rights of Deletion Generally must delete upon receipt of a verified request. Exceptions include:

1. Where needed for Business to perform
2. Detect security incidents, protect against bad acts or prosecute those responsible
3. Identify and repair errors that impair existing intended functionality
4. Exercise free speech or other legal right
5. Comply with CA Electronic Communications Privacy Act
6. For Business internal use reasonably aligned with consumer's expectations on used based on the relationship between the entity and consumer.
7. To comply with legal obligations

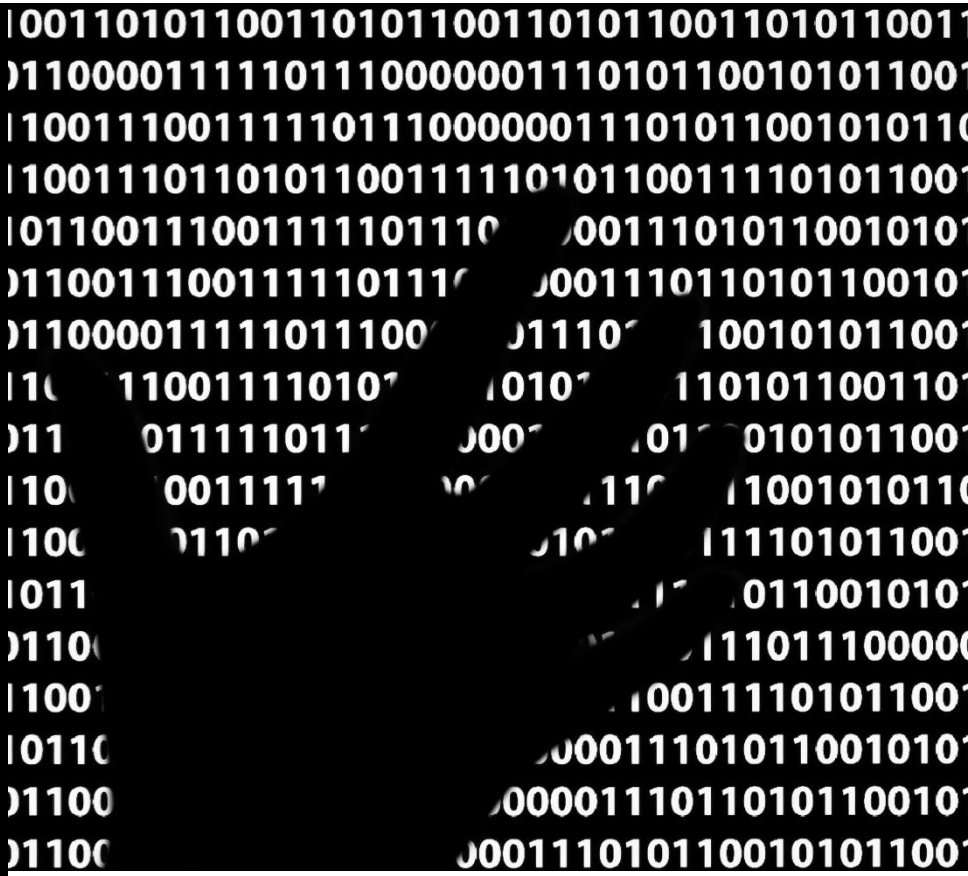
Business Obligation to Consumers

Inform Consumers of collection practices and Consumer rights

No Discrimination against Consumer who exercise their rights

Minimize collection of PI and use thereof

Employee Training



MILES & STOCKBRIDGE

MILES & STOCKBRIDGE

Responding to Consumer Requests

Multiple methods

No charge (unless requests are "manifestly unfounded or excessive")

Respond within 45 days (generally)

Comply with the 12 month look-back

MILES & STOCKBRIDGE

Exceptions to CCPA

1. Where needed to comply with law or government orders
2. To exercise or defend legal claims
3. With respect to PI that is de-identified or aggregated
4. Collect or sell PI if every aspect of the commercial conduct takes place outside of CA
5. Information covered by other federal or state law

Violations

MILES & STOCKBRIDGE

1. Currently private right of action only for data breach
2. Statutory damages
3. Injunctive and declaratory relief
4. Entity has 30 days to cure a breach
5. Consumer Privacy Fund

MILES & STOCKBRIDGE

Comparison to GDPR

MILES & STOCKBRIDGE

One size will not fit all (but both may get you close)!

1. GDPR is an omnibus directive addressing personal data of all EU residents.
    a. Covers disclosures but also covers data security, breach, cross-border transfers
    b. More substance on how Personal Data may be disclosed and what must be shared
    c. Has more individual rights
    d. Requires affirmative consent for processing or opt-in
2. CCPA is focused on the relationship between Businesses and Consumers.
    a. Focus is on the transfer of Consumer PI, including disclosures on transfers
    b. Opt-out process for selling of information

MILES & STOCKBRIDGE

Key Differences

What constitutes Personal Data/Information?

GDPR: Any information relating to an identified or identifiable natural person.

CCPA: Same, but expands the definition to categories such as biometric, commercial information. Includes "household data." There are exclusions for information covered by other federal or state laws, such as HIPAA.

When may Personal Data/Information be processed?

GDPR: When there is a specific lawful basis to do so.

CCPA: Not explicit – CCPA is focused on transparency of what information may be processed and when. Businesses are restricted in when information may be transferred.

MILES & STOCKBRIDGE

Key Differences

Who is subject to the law?

GDPR: Data Subjects are any EU residents. Controllers and Processors must comply with GDPR. There is a two-prong test: First, the business entity must established in the EU (physically or by course of conduct). Second, the entity must control or process the data of EU residents or control or process the data in connection with goods or services provided to EU residents (or to monitor the behavior of EU residents).

CCPA: Consumers are CA residents. Businesses, Service Providers and Third Parties must comply with CCPA. CCPA applies to entities who collect information of Consumers and meet one of the following: annual revenues of more than $25M; buying/selling/sharing for commercial purposes information from at least 50,000 Consumers, households or devices; derive at least 50% of annual revenue from selling information.

MILES & STOCKBRIDGE

Key Differences

What are the Data Subject/Consumer Rights?

GDPR: Right to be forgotten, Right to restrict processing, Right to rectification, Right to data portability, Right to restrict decisions based on automated processing, Right to know who is collecting/processing and why.

CCPA: Right to know who is collecting/processing and why, Right to request deletion of information, Right to opt out of sale of information.

Both statutes have various exceptions, allowing continued collection and processing.

MILES & STOCKBRIDGE

Key Differences

How may Personal Data/Personal Information be transferred?

GDPR: Personal Data may be transferred in compliance with the regulations. The recipient country must provide "adequate assurance" of continued privacy protection. The recipient entity must be able to demonstrate compliance with the adequate assurance of privacy requirements.

CCPA: Personal Information may be transferred without restriction, provided that if the recipient is covered by CCPA, the recipient must comply. Unclear how the transferring entity will verify this, however there must be a written agreement between a Business and its Service Providers.

MILES & STOCKBRIDGE

Key Differences

How is the law enforced?

GDPR: Data Subjects have a private right of action. Regulators may bring enforcement actions, with fines of up to the greater of 20,000,000EUR or 4% of prior year's gross, worldwide revenues.

CCPA: No private right of action, except in connection with data breaches (where statutory damages may be assessed at the greater of $100-750 per consumer per incident or actual damages). Injunctive relief is available. Regulators may bring enforcement actions, with civil penalties of up to $7,500 per violation.

MILES & STOCKBRIDGE

Now What?

MILES & STOCKBRIDGE

The Regs

General Consensus is that the regs go beyond the strict

wording of the statute.

Notices: Initial; Subsequent

Privacy Policies

-Delegation to agents

-Method of communication

The Regs

Right to Know; Right to Delete

-Consumer-specific

Submitting Requests

-Timelines

-Verification Requirements

MILES & STOCKBRIDGE

The Regs

Right to Know; Right to Delete

-Consumer-specific

Submitting Requests

-Timelines

-Verification Requirements

MILES & STOCKBRIDGE

The Regs

Record Keeping

Household Requests

Service Providers

Non-Discrimination

MILES & STOCKBRIDGE

CCPA 2.0

Allister's new ballot initiative:

- Weakens the impact of the amendments to CCPA

- New rights aligned with GDPR

Creates a new CA Privacy Protection Agency

Creates new category of "sensitive" PI

Adds opt-out rights for disclosure and use of sensitive PI

Requires affirmative consent to sell for marketing and advertising purposes (and consumer may subsequently opt out)

New right to correct PI

MILES & STOCKBRIDGE

Will California Lead the Way?

Microsoft announced this month that it will follow CCPA for all United States operations.

Will self-impose these significant restrictions

But, will streamline compliance by having a single U.S. standard

Will other companies follow?

MILES & STOCKBRIDGE

Compliance and Operational Considerations

MILES & STOCKBRIDGE

MILES & STOCKBRIDGE

1. Are you covered by CCPA?
    a. Are you collecting PI from Consumers or receiving PI from a Business?
    b. Are you sharing PI with Service Providers and/or other Third Parties?
2. Disclosures to Consumers
3. Process for Consumer Requests
4. Process Handling Compliance Obligations
    a. Including as to Service Providers
    b. Including as to any applicable financial incentives
5. Prepare for Inquiries and Enforcement

1. Planning and Analysis

a. Inventory and data mapping of PI

b. Confirm processing activities

c. Verify retention/Disposal practices

2. Implementation

a. Develop and implement policies for compliance

b. Develop and implement process for responding to Consumer requests

c. Confirm security procedures against unauthorized access

3. Quality Assurance

a. Conduct risk assessments

b. Review and update policies

c. Implement on-going employee training

d. Also train management and the board

MILES & STOCKBRIDGE

MILES & STOCKBRIDGE

Thank You!

Michele L. Cohen
mcohen@milesstockbridge.com
(410) 385-3449
www.milesstockbridge.com
Twitter: @mstockbridgelaw