90 Days to 2020 -- California Consumer Privacy Act (CCPA), Are You READY?!

October 8, 2019
CCPA Overview

Key Provisions and Definitions
CCPA Snapshot

- Effective January 1, 2020
  - AG enforcement delayed
- Regulates both privacy and data security
- Privacy
  - Consumers have certain rights regarding their Personal Information (“PI”)
    - Rights of information, access, portability, and deletion
    - Right to prohibit the sale of their PI
      - Opt-out rights, except opt-in for under 16
    - Businesses may not “discriminate” for exercise of rights
- Security
  - Businesses must implement “reasonable” data security
    - No significant change from current CA data breach and security requirements, except...
  - Private right of action and statutory damages created for individuals affected by certain types of data security incidents
Effective Date

January 1, 2020

• Possible delay in enforcement of privacy provisions
  – CA Attorney General ("AG") must promulgate regulations by July 1, 2020
  – AG cannot bring enforcement actions until 6 months after publication or July 1, 2020 – whichever date is sooner

• Security provisions effective January 1, 2020
• 12-month “look back” – because consumers must be provided information over the last 12 months of collection, businesses should have begun tracking and recording this information on January 1, 2019
Who Is Protected?

CCPA protects California “Consumers”

(1) Individuals in the State for other than a temporary or transitory purpose; and

(1) Individuals domiciled in the State but outside the State for a temporary or transitory purpose

…however identified, including by any unique identifier
What Data is Covered?

“Personal Information”

Information that identifies, relates to, describes, *is [reasonably] capable of being associated with*, or could reasonably be linked, directly or indirectly, with a particular Consumer *or household*
What is Personal Information?

11 categories

- “Traditional” PII
- Broader Identifiers
  - Unique ID
  - IP address
- Legal Characteristics
- Commercial Information
- Biometric Information
- Internet or Network Activity Information
- Geolocation Data
- Audio, Electronic, Visual, or Similar Information
- Professional or Employment Information
- Education Information
- Other Consumer Characteristics
But it’s not really PII… or is it?!

- **Unique ID:** means a persistent identifier that can be used to recognize consumer, a family or a device that is linked to a consumer or a family, over time and across services, including but not limited to a device identifier, and IP address, cookies, beacons, pixel tags, mobile ad identifiers, customer number, unique pseudonym and user alias. (.140(x))

- **Pseudonymize:** means the processing of PI in a manner that renders the PI no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the PI is not attributed to an identified or identifiable consumer. (.140(r))

- **Probalistic ID:** means identification of a Consumer or a device to a degree of certainty of more probable than not
What is not Personal Information?

- **Excludes** “publicly available” information from public government records
  - BUT, biometric data collected without the Consumer’s knowledge and data used for an incompatible purpose as publicly available may be subject.
  - AB 874 would remove the government purpose limitation (to be approved or vetoed by October 13th)

- **Carve-outs**
  - Protected health information (PHI) governed by CA and federal health information privacy laws
  - To a lesser degree, data regulated by certain other CA and federal privacy laws (e.g., Gramm-Leach-Bliley for financial institutions).
  - AB 25 would also provide a limited temporary carve-out for employment-related information and certain business-to-business communications

- **Unclear** whether “deidentified” data, and “aggregate consumer info” are not subject to “personal information” but they are exempted from some PI limitations and obligations:
  - “De-identified” and “aggregate consumer info” excluded from the restrictions on collection, use, retention, sale and disclosure
  - AB 874 clarifies that deidentified information and aggregate consumer information are not PI
Sale of Data

“Sale”

“Selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.”

Not a “sale” if:

- Consumer directs the transfer and recipient does not sell (unless consistent with the Act)
- Sharing identifier to ensure opt-out
- With a Service Provider or an Exempt Third Party to perform a “Business Purpose” if
  - Explained in privacy notices
  - Contract or certification meets statutory requirements
- Merger/asset sale subject to same use
Business Purpose

The CCPA provides disclosing PI to a SP will not be considered a sale when the use of the PI is for the Business’ or the Service Provider’s operational purposes, or other notified purposes, provided that the use of the PI is reasonably necessary and proportionate to achieve the operational purpose for which the PI was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected and certain contractual protections from the SP are obtained.

Business Purposes are:
- auditing transactions (incl. ad impressions),
- security and fraud prevention,
- protect safety,
- debugging and repairs,
- short-term transient use without profile (contextual customization of ads, not IBA targeting),
- internal research
- performing services on behalf of business or service provider
  ○ Services on behalf of a business include servicing accounts, customer service, processing or fulfilling orders, verifying customer information, payment processing, financing, advertising or marketing, providing analytic services, or providing similar services on behalf of the business.
CCPA Consumer Notices

Overview of Requirements
Notices: Pre-Collection Privacy Notices

With respect to notices, a Business must:

• Provide the categories of PI to be collected and the purposes for which the categories of PI shall be used to Consumers *at or before* the point and time that it collects their PI

• Not collect more and limit the use of PI to the stated purposes, absent further advance notice

• Challenges:
  – Offline
  – Collection not directly from the Consumer (e.g., vendor or data broker)
**Notices**: General Notices vs. Specific Data Requests Disclosures

### General Notices
- **Prior Calendar Year**
- Categories of PI collected;
- Categories of sources;
- Categories of 3P’s with whom the Business shares PI;
- The “Business Purpose” or “Commercial Purpose” for collecting and for selling PI;
- Categories of consumers’ PI sold;
- The categories of consumers’ PI disclosed for a BP.

### Specific Data Requests Disclosures
- **Trailing 12-month look back**
- Categories of PI collected;
- Categories of sources;
- The specific piece of PI collected;
- The categories of 3P with whom the Business shared the PI;
- The “Business Purpose” or “Commercial Purpose” for collection and for selling PI;
- Categories of PI that were sold and the categories to whom the PI was sold;
- The categories of PI disclosed for BP and the categories to whom the PI was disclosed for a BP.
CCPA Consumer Rights

Overview of Requirements
Consumer Rights

Access and Copies Rights
- Consumers can obtain *portable copies* of their information
- The portable copies must be in a readily usable format
- Limited to 2 requests in a 12-month period
- Exception for CA Evidentiary Privileges

Deletion Rights
- Consumers can request *deletion* of their PI being collected from the Consumer by a Business
- Business must direct SP to delete Consumer PI
- No 2x a year limit for requests
- Enumerated exceptions exist, including completing certain transactions or a contract, meeting legal obligations and detecting fraud and security incidents

NOTE: Does not apply to Deidentified Data or Aggregate Consumer Information and no obligation to re-identify
Consumer Rights: Exceptions to Deletion Requests

Businesses are not required to delete information under some circumstances. For example, if the information is necessary to...

- Complete a transaction or perform a contract with the Consumer
- Detect fraud or security incidents or debug and identify errors
- Exercise free speech
- Comply with the CA Electronic Communications Privacy Act
- Engage in certain research activities
- Enable “solely internal uses”
- Comply with a legal obligation
- Otherwise use the information in a lawful manner that is compatible with the context in which the Consumer provided the information
Consumer Rights: Specific Information

Within 45 days of a Consumer submitting a verified request, the Business must associate the info provided by the Consumer to any PI previously collected by the Business about the Consumer in the past 12 months and disclose the following to a Consumer specific to his or her PI depending on whether the Business is collecting, sharing, and/or selling the data:

- The categories of PI the Business has collected about that specific Consumer;
- The categories of sources from which the PI is collected;
- The specific pieces of PI collected about that Consumer;
- The “Business Purpose” or “Commercial Purpose” for collecting and for selling PI;
- The categories of Third Parties with whom the Business shared the PI;
- For PI that was sold, in a separate list, the categories of that specific Consumer’s PI that were sold and the categories of 3Ps to whom the PI was sold;
- For PI that is disclosed for a Business Purpose, in a separate list, the categories of that specific Consumer’s PI that were disclosed for BP and the categories of 3Ps to whom the PI was disclosed for a BP.
Consumer Rights: The Opt-Out Request

• Consumers may direct Businesses to not sell their personal information
  – Aka, the “opt-out” request
  – What is a “sale?”

• To comply, Businesses must:
  – Include a “Do Not Sell” link and other mechanism (toll-free number)
  – Not solicit opt-in or withdraw opt-out for 12 months
Responding to Rights Requests

- Verify the Consumer’s identity
- Identify the type of request (access, portability, deletion, or opt-out)
- Identify relevant information
  - The required disclosure will need to cover the 12-month period preceding the business's receipt of the verifiable consumer request
- Respond within 45 days
  - Subject to some restrictions and extensions
  - Businesses do not have to provide the PI to a consumer more than 2x in a 12-month period
Consumer Rights: Where to Start?

- **Assess current status**
  - Existing capabilities to respond to Consumer rights requests, including determining if exceptions exist
  - Process to review and redact or withhold if permitted
  - Existing recordkeeping processes
  - Identify gaps

- **Augment infrastructure**
  - Leverage data mapping
  - Create platform for logging and responding to requests

- **Inventory sale and sharing practices**
  - Recipient parties
  - Reasons for sale or sharing
  - Abilities to honor opt-out requests

- **Impact on Business?**
Data Discovery and Data Mapping

The Foundations of an Effective Privacy Program
Data Mapping and Analysis May Serve Many Purposes

**Goals**

- Identify Data Repositories/Respond to SARs
- Conduct Privacy and/or Risk Assessments
- Litigation Hold/Preservation Obligations
- Regulatory/Compliance and Monitoring
- Breach Defense, Response, and Asset Protection

**Scope**

- Fact-finding
- Evergreen Data Mapping
- Classification
- Policy Review
- Comprehensive Information Governance
Data Mapping & Information Governance

• Broader Information Governance Questions
  • What can be done with access to the data (i.e., read, write, download)
  • Applicable retention policies
  • Whether the data is used for monetary gain either by first or third parties
  • How individuals can request modification or deletion of their data
Data Mapping & Discovery Sources

- Points of Collection
- Use Cases
- Structure
- Access
- Storage
- Sharing
## Data Mapping & Discovery Sources

| Points of Collection | • Customer/consumer-facing: web forms, account creation, cookies  
|                       | • Internal/employee-facing: applicant data, intranet |
| Use Cases            | • For what purposes is the data collected?  
|                       | • How does the data move around the organization? |
| Structure            | • Elements included (required/optional)  
|                       | • Identifiers (internal and external) |
| Access               | • Who has access to the data, how and why?  
|                       | • Access typically is more extensive than defined use cases (e.g., IT support). |
| Storage              | • Where and how is data stored?  
|                       | • What security controls are in place? |
| Sharing              | • Affiliates, members of the same corporate family  
|                       | • Third parties: service providers v. business partners |
Data Mapping Process Flow

- **Scoping**
  - Assess business processes, workflows and data assets at a high level
  - Determine discovery scope, tools and methods

- **Discovery**
  - Identify and document data assets across organization
  - Collect and evaluate supporting evidence (elements, permissions, data subjects, etc.)

- **Analysis**
  - Synthesize discovery, develop data inventories and workflow maps
  - Identify risks associated with data assets and handling

- **Design**
  - Develop processes and controls to mitigate identified privacy risks
Supporting SAR responses

- What pieces of personal data do you hold about me?
- What personal data about me to you sell or disclose?
Data Mapping/Data Discovery Challenges

- Complexity of systems and maintaining a current data map
- Cultural, political, or bureaucratic barriers to collaboration and sharing
- Mapping confidential or proprietary information
- Identifying all data repositories, whether on-prem, legacy, or cloud-hosted
- Unstructured or semi-structured data can be inconsistently organized, and can span multiple categories
- Different identifiers for different systems
- Inexperience in gathering, vetting, and consolidating the necessary information
- Non-linear workflows
Discovery Tools and Methods

It is critical to deploy the tools and methods most appropriate for the project goals and in context with the in-scope business processes and corporate culture.

- **Interviews/Questionnaires**
  - In person or distributed (by hand or by tool)

- **Technical Analysis**
  - Application and system review and testing

- **Third-Party Discovery and Management Tools**
  - Integrate tools into larger privacy strategy and deploy where appropriate

- **Document Review and Workflow Validation**
  - Review policies, external reps., etc.
  - Run workflows from data subject’s perspective
Project Plan

• Assess and gap analysis
• Map data
• Develop notices
• Create Request Management System
• Train
• Implement
• Reassess and remediate
“Reasonable” Security

- Business operations using sensitive data
- IT systems
- Security threats
- Impact of security events
- Harm to company
- Harm to data subjects

- Policies, procedures, and mechanisms to address identified risks
- Operational, technical and physical

- Documentation of controls in place and how they address identified risks
- Analysis of why certain controls are not needed, and how company is mitigating related risk

- But is it “reasonable”?
“Reasonable” Security

- Generally accepted frameworks provide a strong baseline. For example:
  - NIST 800-53
  - Secure Controls Framework (SCF)
  - ISO 27001, 27002
  - Center for Internet Security (CIS) Controls
  - NIST Cybersecurity Framework

- Security is not “check-the-box,” but…

- For regulators, you should be able to explain why you aren’t checking certain boxes
Use Cases/Questions

• What are “specific pieces”
• How long do I really have to respond?
• How much do I have to do to adequately respond?
• Can I ever charge?
• Can rights be contracted away?
• Whose obligation is .115(d)?
• What about cookies?
About Cyber Solutions

Aon’s Cyber Solutions offers holistic cyber risk management solutions, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

© Aon plc 2019. All rights reserved.


The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

aon.com/cyber-solutions