PAI PRIVACY ASSOCIATES INTERNATIONAL LLC

California Consumer Privacy Act

ISACA & IIA Joint Meeting

December 10, 2019

Keith A. Cheresko, Principal

Purpose of Presentation

- Brief discussion of some of the highlights (lowlights?) of the California Consumer Privacy Act (CCPA)
- High level introduction to some areas of concern for auditors
- Suggestions as to what companies should be doing now

The Legal & Political Privacy Environment

Why did California Enact the CCPA?

- Real Estate Developer Alastair Mactaggart teamed with others and drafted a proposed California privacy ballot initiative in 2016.
- The stated purpose: to "give [Californians] important new consumer privacy rights to take back control of [their] personal information."
- California had introduced legislation in February 2017 focusing on cable and Internet service companies but the bill stalled and was moved to inactive file status on September 16, 2017.
- On October 12, 2017 Mactaggart files "The California Consumer Right to Privacy Act of 2018" with the California AG.

PAI

Time line to enactment of the CCPA

- Signature collection began and by May 2018 over 600,000 signatures are collected
- Fearing voter approval of the ballot initiative, the Legislature offers to pass a sweeping privacy act *if* Mactaggart pulls his initiative
- On June 21, 2018 after 8 months as an inactive file, the dormant CCPA is resurrected and amended so it only could take effect if the ballot Initiative were withdrawn
- The ballot Initiative's proponents agreed to withdraw the ballot initiative
- Thursday, June 28, 2018, California Governor Jerry Brown signed into law what is arguably the most expansive privacy legislation in U.S. history

PAI

Key Timeline Dates

- CCPA is a product of backroom wrangling among legislators, industry, and the primary sponsor of a ballot initiative by the same name
- The CCPA imposes significant and often first-of-its-kind privacy obligations on businesses handling data related to California residents
- The Act is complex and includes drafting errors and ambiguities that are by-products of the speed with which the legislation made its way to the governor's desk
- Some of the kinks were somewhat addressed the amendments adopted in September 2019

PAI

Key Timeline Dates

- January 1 2019 began a 12 month look-back period
- October 2019 required regulations proposed by Attorney General
- January 1, 2020 CCPA goes into effect
- AG enforcement begins earlier of July 1, 2020 or 6 months after final regulation published
- Over time, courts undoubtedly will play a critical role and may have the final say in defining the full scope of the Act and the extent of its obligations

Overview of Some of the CCPA's Key Terms

Are You a Covered Business?

Applies to any entity doing business in California that meets *one* of the following thresholds:

- Annual gross revenues in excess of $25 Million;
- Annually buys, receives for its commercial purposes, sells, or shares for commercial purposes personal information relating to 50,000 or more consumers, households, or devices; or
- Derives 50% or more of its annual revenue from selling consumer personal information

Are You a Covered Business?

Assuming at least one item from prior page is true, your organization is considered a business if *all* of the following are also true:

- You are a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or *financial benefit of your shareholders or other owners*
- You collect consumers' personal information, or someone collects it on your behalf
- You alone, or jointly with others, determine the purposes and means of the processing of consumers' personal information
- You do business in California

What is Personal Information?

Broadly defined as any information that "identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" including in part :

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
- Characteristics of protected classifications under California or federal law.
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information
- Audio, electronic, visual, thermal, olfactory, or similar information.

PAI

What is Personal Information?

- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement
- Geolocation data
- Professional or employment-related information
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99)
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

PAI

What is Not Personal Information?

The statute excludes from the definition:

- Publicly available information
- Protected health information collected by a covered entity as defined under federal laws including HIPAA.
- The sale of information to or from a consumer reporting agency for use in a consumer report consistent with the Fair Credit Reporting Act.
- Personal information collected, processed, sold or disclosed pursuant to the Graham-Leach-Bliley Act or the Driver's Privacy Protection Act of 1994.

PAI

Are Your Customers “Consumers”?

- CCPA applies only if the business collects or sells personal information of consumers
- CCPA defines a “consumer” as a natural person – however identified, including by any unique identifier – who is a California resident

Are Your Customers “Consumers”?

- “consumer” – applies to any business, whether or not geographically located in California, that collects and/or sells the personal information of California residents
- Some limited (1 year) exceptions for applicants, employees, customers, vendors, and individuals associated with commercial customers who are residents of California

Who is a “California Resident”?

The term “California resident” is defined in a separate California statute as:

- Every individual who is in California for other than a temporary or transitory purpose
- Every individual domiciled in California who is outside the state for a temporary or transitory purpose
- Accordingly, if your business collects information from natural persons who live in California, even if they are traveling outside the state when they disclose their personal information, the law applies – except. . .

Extraterritorial Application?

A business is excluded from CCPA scope, even if it collects or sells a consumer's personal information, "if every aspect of the commercial conduct takes place wholly outside of California" such as when:

- The business collected the information while the consumer was outside of California
- No part of the sale of the consumer's personal information occurred in California and
- No personal information collected while the consumer was in California is sold (e.g. a California resident visits a single-source restaurant located outside of California) If California resident makes a restaurant reservation while still in California, that business is included

What is Collect?

- "Collect" is defined as "buying, renting, gathering, obtaining, receiving, or accessing any [PI] from the consumer, either actively, or passively, or by observing the consumer's behavior." (e.g. if a business accesses PI (such as photos or contacts) from a consumer device, it has "collected" PI even if such information is not stored or retained by the business
- A business is considered to "collect" personal information if it buys, rents, gathers, obtains, receives, or even accesses it, by any means, whether actively or passively, including by observing a consumer's behavior
- This definition is clearly intended to extend to online monitoring and tracking

PAI

What is “Sale” or Selling”?

- A CCPA “sale” is disclosing PI to “another business or third party for monetary or other valuable consideration.”
- Unclear how broadly courts will interpret “valuable consideration”
- Interpretation critical because the definition of “sale” defines, among other things, the scope of the consumer opt-out right provided.
- “Selling” consumer personal information takes place upon “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means” for “monetary or other valuable consideration.”
- The definition contains exclusions for consumer consent; conveying a consumer’s opt-out instructions to a third party; or data transfers in the course of mergers, acquisitions, bankruptcies and the like

PAI

What is Not “Selling” and “Business Purposes”?

- “Selling” excludes use for a “business purpose”, defined as using personal information for the operational purposes of the business or its service provider, as long as “reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed” or for another compatible operational purpose
- CCPA lists seven specific “business purposes” that include:
  - things as counting ad impressions
  - detecting security incidents
  - debugging and repairing functionality
  - short-term “transient use” that isn’t used for profiling
  - performing services on a business’s behalf, such as fulfilling orders or processing payment (classic “data processor” activities)
  - undertaking internal research for technological development
  - undertaking activities to verify or maintain the quality or safety” of the business’s service or device

PAI

What is a “Service Provider”?

A for-profit entity that processes information on behalf of a CCPA-covered business, where the covered business:

- Enters into a written contract with the entity prohibiting the entity from undertaking any processing of the personal information other than for the specific purpose of performing the services specified in the written contract
- Obtains “certification” that the entity understands the restrictions
- When requested, the entity must delete personal information it processes for the CCPA-covered business, subject to the same exceptions to the right to delete as the covered business
- The entity is liable for its own violations of CCPA, and the business that discloses the personal information to the entity also will be liable for the entity’s CCPA violations if the business had “actual knowledge or reason to believe” that the entity intended to violate CCPA

What Privacy Rights Do Individuals Have?

CCPA Individual Privacy Rights

- Right to Know
- Right to Access
- Right to Deletion
- Right to Opt Out
- Right to Opt In for Consumers Under Age 16
- Right to Equal Service and Price

Right to Know

- A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected
- A business that collects a consumer's personal information shall, at or before the point of collection:
- inform consumers as to the categories of personal information to be collected
- the purposes for which the categories of personal information shall be used
- A business shall provide the information to a consumer only upon receipt of a verifiable consumer request.

Right to Know

- A business that receives a verifiable consumer request from a consumer to access personal information shall:
- Promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section.
- May be delivered by mail or electronically, and if provided electronically,
  - the information shall be in a portable and,
  - to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance

Right to Know

Verifiable consumer request process changes

- No toll-free number
- Operate exclusively online + have a direct relationship with consumers, who do not need to provide a toll-free phone number.
- Existing account usage. Can require consumers to use an existing account.
- Verification criteria. “Reasonable in light of the personal information requested.”
- Categories not entities (still individualized?).
- Categories: sold + third parties

Right to Know

- Business not required to provide personal information to a consumer more than twice in a 12-month period
- Does not require a business to:
- Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.
- Re-identify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

Right to Know

- Requires businesses to make available two or more designated methods to request the information, including at a minimum, a toll-free number and, if the business has a website, a website address
- Must disclose certain information about CCPA rights online, including, if applicable, in its online privacy policy or in any California-specific description of consumers' privacy rights
- This information must be updated at least once a year, and includes:
  - a description of rights under the Act
  - a list of categories of PI collected, sold to a third party
  - disclosed for business purposes

Right to Access

Right to receive information about, and Copies of, PI

- If asked by a consumer, a business must disclose the categories of PI that the business, within the year preceding the request, has:
  - collected
  - "sold" to a third party
  - disclosed for a business purpose
  - the categories of third parties to whom the Business sold and/or disclosed PI for a business purpose
- Plus requires that a business also disclose:
  - the business or commercial purpose for which PI was collected and/or sold
  - the categories of sources from which PI was collected and
  - the "specific pieces" of PI a business collected about an individual

Right to Delete PI

- CCPA provides consumers with a right to request a business delete any PI that it has collected about the consumer and the business must direct service providers to delete a consumer's PI in response to a verified "deletion" request
- There are exceptions to the obligation to delete such as:
  - completing a transaction,
  - detecting security incidents,
  - debugging to repair intended functionalities
  - where PI is used "to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business,"
  - where a business "otherwise use[s] the consumer's [PI] internally in a lawful manner that is compatible with the context in which the consumer provided the information."

Right to Opt Out

- The right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information.
- A business that sells consumers' personal information to third parties shall provide notice to consumers that this information may be sold and that consumers have the right to opt out of the sale of their personal information.
- A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

Right to Opt Out

- A business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information.
- A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt in."
- CCPA requires a "clear and conspicuous" link on the business's homepage titled "Do Not Sell My Personal Information," as well as a link to the business' privacy policies
- If the business has a separate page for California consumers and takes reasonable steps to direct Californians to that page, the business does not have to include the "Do Not Sell" link on its homepage

Right to Be Free from Discrimination

- Prohibits businesses from charging different prices or rates to consumers, providing different services, or denying goods or services to consumers who exercise their CCPA rights
- Exceptions are permitted for example, where the difference in prices or services is reasonably related to the value to the business provided by the consumer's data
- The Act also allows businesses to offer financial incentives in connection with the collection, sale, or deletion of PI
- Consumers must opt-in to such programs, and a business must include a description of the program on its "Do Not Sell My Personal Information" page

Exceptions to Deletion Requests

- Where complying with the Act would interfere with compliance legal processes
- For collections “wholly outside” California
- Where compliance would violate an evidentiary privilege, such as the attorney-client privilege
- For certain information covered by other state and federal privacy laws, although these exceptions often only will apply to the extent the Act “conflict[s]” with the federal privacy law, such as the Gramm-Leach-Bliley Act.
- The true scope and impact of these exceptions will become clearer as businesses analyze the Act’s requirements on specific processes and procedures and assess the extent to which those requirements impede or restrict business operations.

How is CCPA Enforced?

Private Right of Action

- CCPA grants a private right of action to individual Californians
- Any natural person with California residency has a right of action if their unencrypted or un-redacted personal information has been exposed due to a business's failure to maintain appropriate security safeguards
- Note that the definition of personal information in this section is not the definition found in the remainder of CCPA
- The definition is sufficiently narrower and limited to a person's name (at least first initial and last name) and either their social security number, driver's license or state identification number, bank or credit card information, or medical or health insurance information.
- A breach involving data that is encrypted or redacted is not subject to the CCPA's private right of action

PAI

Private Right of Action

- There is no pecuniary damages requirement
- Plaintiffs can seek statutory damages between $100 and $750
- Injunctive or declaratory relief; or “any other relief the court deems proper”
- Actual damages are only recoverable if they exceed the statutory damages
- Actions can be aggregated into a class action
- Two checks on Private enforcement
  - The action is subject to the same notice requirement as its public counterpart. Prospective plaintiffs, except those pursuing an individual action for pecuniary damages, must give a prospective defendant business written notice of the intended action and 30 days to cure the problem. The action can only proceed if the company fails to fix the problem within the time allotted.
  - Second, the California attorney general has the authority to stop or superintend a private action. Within 30 days of filing the action, after the chance to cure has elapsed, the plaintiff must notify the attorney general’s office.

PAI

State Enforcement

- A business shall be in violation for failure to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be liable for a civil penalty as provided in in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.
- Any person, business, or service provider that intentionally violates this title may be liable for a civil penalty of up to seven thousand fine hundred dollars ($7,500) for each violation.
- It is the intent of the Legislature that the percentages specified in subdivision (c) be adjusted as necessary to ensure that any civil penalties assessed for a violation of this title fully offset any costs incurred by the state courts and the Attorney General in connection with this title, including a sufficient amount to cover any deficit from a prior fiscal year.

PAI

What to do?

- Review and update your public facing web documents
- Consumer privacy policies
- Website usage
- Services
- Job applicant privacy policy
- Review your public facing website to ensure that it does not contradict with your privacy policy terms

What to do?

- Update internal policies
- Employee privacy notices
- Training
- Vendor compliance
- Vendor contract policy
- Data security addendums
- Template contract language

What to do?

Plan for verifiable consumer requests

- Web form
- Toll-free number
- Draft response letters
- Process for responding to “you must comply” letters from customers and supply chain participants

Contact Information

Keith A. Cheresko

Privacy Associates International LLC

kcheresko@privassoc.com

www.privassoc.com

(248) 535-2819