

CCPA Litigation Avoidance for Companies in 2020 and Beyond



Meet the Panelists

Moderator: Andrew Bayer, CEDS; Inventus – Managing Shareholder

Panelist: Erin Plante, PMP, CAMS; Inventus – Director, Strategy and Consulting

Panelist: Natalie Prescott, Esq., CIPP/US; Mintz Levin - Associate

Panelist: Travis Stewart, Esq.; Lytx – Senior Counsel

Covered in this Presentation

Overview of CCPA

CCPA Obligations by Entity Type

CCPA Consumer Rights

Legislative Updates

Enforcement of CCPA

Litigation Avoidance

CCPA Compliance and Risk-Reduction Strategies

What's Next?

Overview of CCPA



CCPA: The Basics

The California Consumer Privacy Act (CCPA or AB 375) is a piece of consumer privacy legislation which at its core, gives more power to the consumers over their private data. Passed into CA Law in June of 2018 and takes effect January 1st, 2020.

Two Main Groups Identified in Bill Are:

Businesses – For-profit which does business in California, collects personal information of their consumers and is ONE of the following:

1. Has annual revenues in excess of \$25M
2. Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices
3. Derives 50% or more of it's annual revenues from selling consumers' personal information

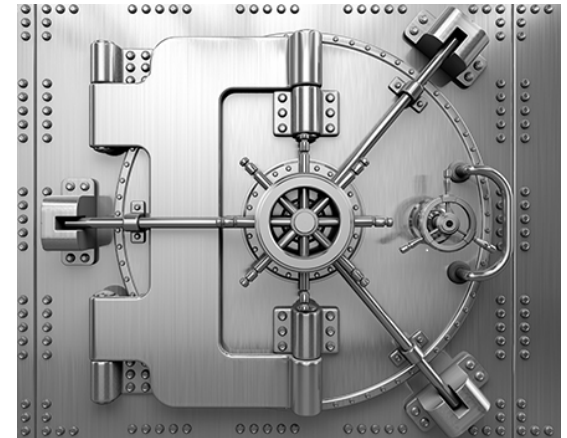
Consumers: “a natural person who is a California resident as defined in section 17014 or Title 18 of the California Code of Regulations.”

Who is a “Consumer”?

- A “**consumer**” is “a natural person who is a **California resident**, as defined in Section 17014 of Title 18 of the California Code of Regulations . . . , however identified, including by any unique identifier.”
- Per these state regulations, a **California resident** is any individual who is (1) “in the state of California for other than a temporary or transitory purpose,” or (2) “domiciled in the state” of California and “outside of the state for a temporary or transitory purpose.”
- This is a broad definition. Note that a Consumer does not need to be engaging in a commercial activity to be a consumer.
- Personal Information originates from a Consumer. Understanding the data flow will require understanding who the Consumer is.

What Is “Personal Information”?

- **Personal Information** is defined as “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”
 - *The term "household" is not defined. It could include residences outside of the state of California where a California resident is currently housed, as well as any connected devices within those households that contain Personal Information about California residents.*
- CCPA includes examples of **Personal Information** such as: commercial information, purchase histories, internet and network activity including search history, browsing history, interactions with apps, websites, or advertisements, geolocation data, or profiles created from other Personal Information about a consumer.
 - *On August 31, 2018, via SB-1121, the California State Legislature made certain amendments to the CCPA. One of these was to clarify that these categories would only be **Personal Information** where they were linked or linkable to a Consumer or household.*



Overview of CCPA: Does Not Apply to Aggregate Consumer Information or Deidentified Data

- If data is “deidentified” such that it cannot be linked to a specific consumer, then it becomes “deidentified data” and CCPA does not apply.
- CCPA requires the use of technical safeguards and business processes to be used to prevent reidentification of this type of data.
- Similarly, CCPA does not apply to “aggregate consumer information” defined as “information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.”
- When designing a business process or data flow, always consider whether deidentified or aggregate data could serve the business purpose.



Overview of CCPA: Collecting and Selling Personal Information

- Does Your Entity Collect Consumer Personal Information?
 - If your entity **buys, gathers, rents, obtains, receives, or even accesses** Consumer Personal Information, by any means, whether actively or passively, including by **observing a Consumer's behavior**, then it is collecting Consumer Personal Information.
- Is Your Entity Selling Personal Information?
 - Selling of Consumer Personal Information will occur where your entity is “**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]” for “monetary or other **valuable consideration.**”

CCPA Obligations by Entity Type



CCPA Entity Types – Understanding the Relationships Between the Three Entity Types

- CCPA imposes burdens on three different types of entities:
 - Businesses
 - Service Providers
 - Third Parties
- A given entity could fall under all three categories, depending on its activities. Many entities will have more than one type of data flow subject to CCPA.
- Many Service Providers may also be Businesses under CCPA because of employee information.
- In GDPR terms, a Business is the Controller, and the Service Provider is the Processor.

Is Your Entity a “Business”?

- Are **each** of the following true?
 - Your entity **collects Personal Information from Consumers**, or another entity collects it for you.
 - **You determine**, or do so with others, **the purpose and reason for processing Consumer Personal Information**. Note this is a key distinction between Business and Service Providers. Service providers take their instructions from the Business.
 - **You do business in California**. While not defined by the CCPA, it is reasonable to assume that this would apply to any business who collects Personal Information from a Consumer. Thus, the Business does not need to be geographically located in California.
- Are **one or more** of the following true?
 - You have annual gross revenues in excess of \$25,000,000.
 - You annually buy, share or receive for commercial purposes, or sell, the **personal information of more than 50,000 consumers**, including households and devices.
 - You receive 50 percent or more of your annual revenue from selling of consumers' personal information.

Is Your Entity a “Service Provider”?

- **Service Providers** are entities that “**processes** information **on behalf of a business** and to which the business **discloses** a consumer’s **personal information** for a business purpose pursuant to a **written contract.**”
- The written contract must prevent the Service Provider from “from retaining, using, or disclosing personal information for any purpose,” other than that of performing the services provided for by the contract.
- Further, Businesses must obligate their Service Providers to “direct any service providers to delete the consumer’s personal information from their records” when a consumer requests that the Business do so.

Is Your Entity A “Third Party”?

- CCPA describes what a “third party” is not.
- A “Third Party” is any entity that is not a CCPA Business, nor a Service Provider, but **still receives a Consumer’s Personal Information** from the Business.
- Consumers can only opt out of the providing of their Personal Information to Third Parties, not Service Providers.
- Third Parties cannot sell Personal Information about a Consumer sold to it by a Business unless the Consumer has been provided explicit notice regarding the opportunity to opt out of the sale.



CCPA Consumer Rights



CCPA Provides Rights to California Residents

- The CCPA talks about “consumers.”
- A “**consumer**” is “a natural person who is a **California resident**, as defined in Section 17014 of Title 18 of the California Code of Regulations . . . , however identified, including by any unique identifier.”
- Per state regulations, a **California resident** is any individual who is (1) “in the state of California for other than a temporary or transitory purpose,” or (2) “domiciled in the state” of California and “outside of the state for a temporary or transitory purpose.”
- If the customer is not a California resident, the CCPA will not apply to that customer’s actions activity directly.
- Consider whether segmenting out California residents is possible from a technical and business perspective.

CCPA: Individual Rights

- Under the CCPA, California residents have specific rights with respect to their personal information.
 - **Access and Portability** – Right to request that a business collecting an individual’s PI disclose to the individual the categories and specific pieces of PI that the business has collected
 - **Deletion** – Right to request that a business delete any PI about the individual which the business has collected from the individual
 - **Opt-Out** – Right, at any time, to direct a business that “sells” PI about the individual to third parties, not to “sell” that person’s PI (Business must provide opt-out mechanism on homepage)
 - **Non-Discrimination** – Right to non-discrimination (pricing, quality or quantity of goods sold, etc.) by a business solely because the individual chooses to exercise any CCPA rights
 - **Notice/Disclosure** – Right to receive full notice/disclosure regarding (a) when collecting PI, categories of data (PI, sources, 3rd parties), business purpose, and specific PI and (b) if a business “sells” PI to third parties, or otherwise discloses PI for a business purpose, categories of data (PI collected/sold, 3rd parties sold to, business purposes)

Individual Rights

- These rights apply to all Personal Information collected from Consumers by a Business.
- Service Providers will need to be able to support these rights.
- Businesses need to be able to ensure their processes and contracts will enable them to meet these requirements.
- Third Parties will want to protect themselves via contract and due diligence as to any data they receive.

Rights: Disclosure/Privacy Policy Requirements

- Before or at the time of collection, a Business must:
 - Inform Consumers of the categories of Personal Information to be collected.
 - Inform Consumers of the purposes for which the categories of Personal Information shall be used.
 - Provide notice of the collection of any additional categories of information or use of collected information for any additional purposes taking place after initial disclosures have been made.
- Privacy Policy Requirements
 - A listing of Consumers' rights under the CCPA, including the consumer right to opt out of the sale of the Consumer's Personal Information and a separate link to the "*Do Not Sell My Personal Information*" on the Business's website.
 - How Consumers may submit requests to exercise their rights to the Business.
 - A list of the categories of Personal Information that the Business has collected about Consumers, sold about Consumers, and disclosed about Consumers for a business purpose in the preceding 12 months.

Legislative Amendment Update



2018: Key Amendments

- SB 1121 passed on August 31, 2018.
- SB 1121 clarified certain CCPA exemptions:
 - Data covered by other privacy frameworks such as **HIPAA** or the **Graham-Leach-Bliley Act**
 - **Non-profit** entities
 - PHI collected by a **covered entity or business associate**
 - Medical information governed by the California Confidentiality of Medical Information Act (**CMIA**)
 - Information collected as part of a **clinical trial** subject to the Common Rule, ICH Good Clinical Practice Guidelines, or FDA Human Subject Protection Regulations



2019: July 7th Senate Judiciary Committee Hearing

- Major (12-hour) hearing to move bills from committee to Senate floor
- Senator Hannah Beth-Jackson supported two “clean-up” bills, without requesting amendments.
- Both bills sailed through committee are likely to become law.

2019 Consensus Bills



AB 25 – Employee Data

- AB 25 was proposed to **carve out employee data from the CCPA definition of “personal information.”**
- As amended in the Senate, AB 25 now provides a **one-year moratorium for most CCPA requirements for employee**, job applicant, contractor, beneficiary, and emergency contact information
- PROVIDED that information is used SOLELY in employment context
- ISSUE #1: If an employee (or applicant, contractor, etc.) is also a **consumer of the business outside the employment context**, all personal data collected in the consumer context remains covered by CCPA
- ISSUE #2: **Data collected by third parties at the employer** for “voluntary” activities, such as fitness programs. If this activity information is provided to a marketing or insurance company and then used to offer the employee any sort of **service outside the work context** (including discounts), that would be regulated by the CCPA.

AB 25 – Employee Data

- This is a one-year “moratorium” on the application of the broader scope of CCPA to “employee data,” agreed to by representatives of the labor unions and the California Chamber of Commerce.
- Two CCPA requirements will continue to apply to this range of “employee data.”
- Employers **must provide employees** with CCPA Section **1798.100(b) privacy notices**.
- CCPA **private right of action** under Section 1798.150 will **apply to employee data**.
- TAKEAWAY FOR EMPLOYERS
 - **Include mapping of employee data** in CCPA data-mapping exercises to provide an accurate notice.
 - Mapping critical for accurate and complete data breach response to remediate damages under Section 1798.150.
 - Unions and C of C intend to work together to develop **legislation to address intrusive employee monitoring**. Consider **waiting until Q4 of 2020 to adopt new employee-monitoring techniques**.

AB 25 – Guidance on Verifying CCPA Rights Requests

- Another amendment to AB 25 contains language clarifying that for all California resident requests other than “do not sell” requests businesses may require authentication that is **“reasonable in light of the nature of the personal information requested.”**
- Further clarifies that, although the CCPA prohibits businesses from requiring a resident to create an account with a business in order to submit a request, **if the resident already has an account, the business may require the resident to submit the request through that account.** This will help businesses with “customer portals” or “customer dashboards” to utilize that functionality.
- The AG must issue regulations clarifying the procedure for verifying California resident requests.
- This “authentication” language in AB 25 provides a useful preview for beginning to plan how to handle CCPA requests.

AB 874 – Expanding the Public Record Exception

- As originally passed, the CCPA denies a “public records” exception for any use of public record information **“for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.”** Section 1798.140(o)(2).
- Language drew criticism for being unclear and potentially violating the First Amendment.
- CCPA sponsor Alastair McTaggart expressed concern that it might be struck down as unconstitutional.
- AB 874 removes this limitation; it cleared Senate Judiciary on a consent vote.
- Note: although the Section 1798.140(o)(2) exception uses the term “publicly available data,” it **defines the term only as public/government record data**. In practice, this means that information that is publicly available (e.g., posted online, directory, etc.) is unlikely to be exempt unless it is also public/government record data.

2019 Bills Passed With Amendments



AB 846 – Loyalty Program and Premium Features Clarification

- As amended in committee, AB 846 has been **scaled back** significantly.
- The Senate amendment (like the Assembly version) clarifies that **businesses can still offer consumers a different rate, price, level or quality of goods** to a consumer who has exercised any of the consumer's CCPA rights so long as:
 - The offering is in connection with a consumer's **voluntary** participation in a loyalty, rewards, premium features, discounts, or club card program; and
 - The terms of the program are not “unjust, unreasonable, coercive, or usurious in nature.”
- Senate bill now states that the bill has **no effect on “do not sell” rights** under the CCPA
 - Businesses must offer the program even if a consumer opts out of the “sale” of their data
- Also eliminates coverage of “free” programs whose functions “are directly related to the collection, use or disclosure of personal data,” which had been included in the Senate bill.
- Committee also voted in principle to ban businesses offering these loyalty programs from “selling” the personal information gathered as part of the program. Unclear if the bill as amended will become law at all

AB 1546 – CCPA toll-free number requirement

- AB 1564, which passed the Assembly unanimously, **exempts businesses that operate exclusively online from the requirement to maintain a toll-free number** for purposes of requests under the CCPA
- Bill allowed online businesses to provide an **email address in lieu of the toll-free number.**
- AB 1564 passed the Senate Judiciary Committee with a narrowing amendment, limiting the exception to **businesses that have a direct relationship with the California residents** from whom it collects personal information.
- Also requires that if the online business maintains a website, the business must provide a method to submit requests **through that website.**

AB 1146 – Auto warranty, repair, and product recall exemption

- AB 1146 passed the Assembly, exempting from the CCPA opt-out requirement any vehicle or ownership information retained or shared between a new motor vehicle dealer and the Original Equipment Manufacturer (“OEM”), as defined in Section 672 of the Motor Vehicle Code.
- Limitation – if the information is **shared for the purpose of effectuating or in anticipation of effectuating a vehicle repair** covered by a vehicle warranty or recall.
- Senate amendment **strictly limits any selling or sharing** of the information **for any other purpose**.

Status of Remainder



Significant Failures to Proceed

- SB 561 – Introduced the **private right of action** for any violation of the CCPA. This bill failed to make it out of committee and is considered dead for the session.
- AB 288 – Included the **right to request permanent deletion and prohibition on future sale** of personal information upon account closure. The hearing for this bill was canceled at the request of the author and it did not proceed.
- AB 1760 – “Privacy for All.” Significantly changed the CCPA’s provisions to include affirmative **opt-in consent to share** personal information. The hearing for this bill was cancelled at the request of the author and did not proceed.
- AB 873 – would **amend the CCPA definition of “de-identified” data** to align it with the Federal Trade Commission’s 2012 Privacy report. Was blocked in the Senate Judiciary Committee.
- AB 1416 – would have created **an exemption from the CCPA on “do not sell” rights for sales of information to governments** to further government services **and sales of information to private sector customers for antifraud, cybersecurity and detection of illegal activity**. Bill was withdrawn before the hearing.

Others

- AB 950 – discloses **monetary value of consumer data**. Did not pass out of Assembly.
- AB 981 – would **eliminate a consumer's right to request a business to delete or not sell** consumer's personal information if it is necessary to complete an **insurance transaction**. Did not pass out of Assembly.
- AB 1416 – established various **exceptions to the obligations of a business' ability to collect, use, retain, sell, or disclose** personal information. Hearing cancelled at request of the author.
- SB 753 – **exempts certain data sharing** related to targeted advertising **from** CCPA **"do not sell"** compliance requirements. Hearing cancelled at request of the author.

Legislative Calendar



Remaining Calendar for Action

- **August 30**: last day for fiscal committees to report bills to the floor.
- **September 13**: last day for the Senate to vote bills into law.
- **October 13**: last day for the governor to sign or veto bills that survived the Senate.

Enforcement of CCPA



Enforcement: CA Attorney General

- **CA Attorney General**
 - **Violations Generally:** Authority to bring action for up to \$2,500 for any violation of CCPA.
 - **Damages:** Calculated on a per-capita basis. For example, if a violation affects 1,000 users, damages could rise to \$2,500,000.
 - **Intentional Violations:** For violations viewed as intentional, the Attorney General's office may bring an action for up to \$7,500 for any violation of the CCPA. The same 1,000 users could be awarded damages of \$7,500,000.
 - **Notice and Cure Period**
 - Entity has 30 days after receiving notice of noncompliance from the California Attorney General's office to cure it, and only thereafter are they subject to an enforcement action for violating CCPA.

Enforcement: Private Right of Action

- **Private Right of Action**

- **Consumer:** May bring civil action for alleged failure to “implement and maintain reasonable security procedures and practices” by Business that results in a data breach of non-encrypted or non-redacted Personal Information.
- **Individual or Class Action:** Action may be brought as class action or on an individual basis.
- **Damages:** CCPA provides for statutory damages between \$100 and \$750 or actual damages.
- **Notice and Cure Period:**
 - Consumer must provide Business 30 days to cure the alleged violation.
 - If the Business actually cures the violation within 30 days, no action may be initiated.
 - No notice shall be required prior to an individual Consumer initiating an action solely for actual damages suffered.
- **SB 561:** This controversial bill did not make it out of Senate this season. It threatened to expand the Act’s private right of action by allowing consumers to bring actions when any of their CCPA rights were violated.

Litigation Avoidance and Risk Reduction



CCPA Will Change Your Business in 3 Ways:

1. Customer-Facing

- The CCPA grants your customers who are California residents certain rights.
- Customer-visible changes will include privacy policies, website data collection mechanisms, customer-facing mechanisms for exercising rights such as access and deletion, a “Do Not Sell” link, and more.

2. Internal Process Alignment

- Supporting CCPA rights granted to Consumers will require creating and retooling existing internal processes.
- This would include being able to support data access and portability, opting out of the sale of one’s Personal Information, and also the non-discrimination provision generally.

3. External Process Alignment

- CCPA requires that Businesses impose obligations on their Service Providers to enable them to support Consumer rights, and put obligations on Businesses that sell Personal Information to Third Parties as well.

Compliance Strategies: Questions to Ask

- Non-discrimination and financial incentives are likely to be most complex areas for compliance purposes.
- **How are you** currently **using** Personal Information to offer goods and services?
- What would happen if you had to delete some of that information because a Consumer asked you to?
- **If a Consumer opted out** of the sale of their Personal Information, which information transfers would you have to stop making? Could these transfers still be effectively done if a significant portion of Consumers opt out?
- CCPA has a limited exception to deletion to combat fraud. **Would your existing anti-fraud mechanisms still work** if a Consumer asked to delete their Personal Information and opted out of the sale of their data?
- Does your Business need or **derive appropriate value from all of the personal data** it collects? Could it achieve its goals with less liability and compliance burden if it chose to collect less?
- How would the offering of **financial incentives** to the Consumer for the collection or sale of Personal Information **impact the viability** of the Business?
- Culturally, how does the Business plan to make CCPA **compliance a priority while demonstrating its value** to stakeholders?

Compliance Strategies: Critical Steps

- **Understand how Personal Information flows** through your organization.
- **Points of Collection:** Has **privacy policy** been **updated** to disclose what information is being collected, disclosed, and sold? Does it disclose the right to opt-out of any such selling? Does it explain the new Consumer rights provided by the CCPA?
- **Data Management:** Complying with the CCPA will require understanding **where Personal Information is** at any given time. Companies will need **mechanisms to track business processes, products, devices, applications and third parties** that access the Personal Information of Consumers.
- **Support for Consumer CCPA Rights:** The rights of Access/Data Portability, Deletion, Opt Out Requirements/Non-discrimination will require support throughout the organization, and at the information technology infrastructure level.
 - **Consumer Requests:** Verify, document, and support requests.
 - **Create Systems of Record:** This will serve as a record of the execution of Consumer requests.
 - **Provide Training:** Stakeholders must be informed and empowered to act.
 - **Testing:** Test processes and controls before January, 2020.

Compliance Strategies: Focus on Security

- **Information Security:** Identify and **close any security gaps**.
 - The CCPA will greatly **increase the cost of non-remediated gaps** through its statutory **damages** provision within the private right of action.
 - Being able to **track where data was, and attest that it was not breached** will be important for limiting exposure.
- **Service Provider Agreements:** Create a **process for reviewing current and future contracts** and negotiating necessary **CCPA amendments**. Remember that if appropriate provisions are not in place, there is the possibility that the vendor may not be considered a Service Provider under the CCPA.
 - Service Provider **must refrain “from retaining, using, or disclosing** personal information for any purpose,” other than that of performing the services provided for by the contract.
 - Service Provider **must agree to support Consumer CCPA rights**, including Access/Portability, Deletion, and Opt-outs.

What to do before 2020? Is there still time?

- Take a look at your data and your data sets
- Figure out where personal information is located and how it is being processed
 - Consider a data-mapping exercise
- Evaluate potential CCPA applicability
- If CCPA applies, establish a plan for responding to requests from California consumers to access their personal information, have their personal information deleted and otherwise exercise their rights under the law
- Arbitration Clause
- Class Action waiver

Customer-Facing CCPA Compliance



Customer-Facing: Understanding Your Information Surfaces

- **Take a holistic view of how CCPA Consumers can interact with your Business:**
 - Websites
 - Apps, including through the Google and Apple stores
 - Mechanisms in physical stores, including tracking of devices, paper forms, and loyalty programs
 - Kiosks, including self-service stations
 - Each of these mechanisms may present their own challenges
- **Always consider three areas for customer-facing information surfaces:**
 - Notice
 - Non-Discrimination
 - Financial Incentives

Customer-Facing: Notice Generally

- **Before or at the time of collection, a Business must:**
 - Inform Consumers of the categories of Personal Information to be collected.
 - Inform Consumers of the purposes for which the categories of Personal Information shall be used.
 - Provide notice of the collection of any additional categories of information or use of collected information for any additional purposes taking place after initial disclosures have been made.
- **Privacy Policy Requirements:**
 - A listing of Consumers' rights under the CCPA, including the Consumer right to opt out of the sale of the Consumer's Personal Information and a separate link to the "Do Not Sell My Personal Information" on the Business's website.
 - How Consumers may submit requests to exercise their rights to the Business. This will include access/portability rights and deletion rights.
 - A list of the categories of Personal Information that the Business has collected about Consumers, sold about Consumers, and disclosed about Consumers for a business purpose in the preceding 12 months.

Customer-Facing: Notice Issues For Information Surfaces

- **Websites:**
 - Ensure that the privacy policy provides adequate disclosure, based on expansive definition of Personal Information, and includes "Do Not Sell My Personal Information" where appropriate.
- **Apps, including through the Google and Apple stores:**
 - Ensure that the privacy policy is consistent with what you have said and explained in your website policy. Pay attention to disclosing additional or different collection of Personal Information, including location tracking, device activity and others.
- **Mechanisms in physical stores, including tracking of devices, paper forms, and loyalty programs:**
 - Consider what mechanism will be appropriate to provide notice. Some aspects of information collection, such as the use of devices that track Consumer cell phones, may create novel notice issues.
 - How will your loyalty program be implemented?
- **Kiosks, including self-service stations:**
 - Ensure that the privacy policy covers the functionality provided. If additional information collection mechanisms are present, these must be appropriately disclosed.

Customer Facing: Non-Discrimination and Financial Incentives Generally

- Non-Discrimination
 - Businesses are prohibited from discrimination against Consumers for exercising their CCPA rights, including:
 - Denying Consumers goods or services;
 - Charging different prices or rates for goods or services, including through the use of discounts, benefits, or other penalties;
 - Providing a different level or quality of goods or services; and
 - Suggesting that a Consumer will receive a different price or quality of goods or services if the Consumer exercises rights under the law.
- Businesses may charge Consumers different prices or offer different levels of service if the difference is “reasonably related to the value provided to the consumer by the consumer’s data.”
- Further, Businesses may offer financial incentives, including payments to Consumers as compensation for the collection, sale, or deletion of Personal Information, if:
 - The programs are not “unjust, unreasonable, coercive, or usurious in nature,” and
 - The Business obtains opt-in consent prior to enrolling a Consumer in a financial incentive program, and provides Consumers with the opportunity to revoke consent for such programs at any time.

Customer-Facing: Anti-Discrimination Issues For Information Surfaces

- **Websites**
 - Pop-up discount offers
 - Register for promotions
 - Offering different promotions/pricing based on what you know about a specific Consumer (Consumers may have exercised right of deletion and not get the same deals)
- **Apps, including through the Google and Apple stores**
 - How does the app use gathered information to provide different goods or services to different Consumers?
 - User turns off location permissions and is not offered certain deals
 - User does not apply access to social media platforms and is not eligible for certain promotions
- **Mechanisms in physical stores, including tracking of devices, paper forms, and loyalty programs**
 - User follows instruction to opt of out device tracking via posted notice by turning off Bluetooth and is not offered certain deals
 - How will your loyalty program be structured?
- **Kiosks, including self-service stations**
 - What if functionality is only provided after the user provides Personal Information such as an email address, the information is not necessary to provide the requested functionality, and this is the only on premise way to accomplish the task?

Customer-Facing: Anti-Discrimination Questions

- What can Consumers do differently if they provide our entity with Personal Information?
- How do we treat Consumers differently based on what we know about them?
- What is the “value provided to the consumer by the consumer’s data”?
- Should we restructure one or more of our collection mechanisms as an opt-in financial incentive?
- Are there potential unjust or unreasonable aspects that need to be considered?

CCPA Compliance and Risk-Reduction Strategies



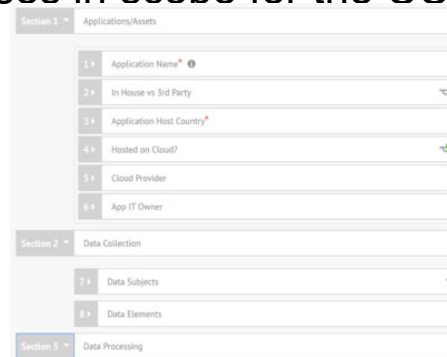
CCPA Compliance: Know Your Data

- Covered Business Processes
 - Identify all your businesses processes in scope for the CCPA:
 - Are you a business?
 - Are you a service provider?
 - Are you both?
- Data Mapping
 - Prerequisite to ensuring reasonable security procedures are in place.
 - Use data map to create Records of Processing, including formal inventory of data processing operations and supporting systems that collect, process and store CA resident PI.
 - Enables effective response to consumer requests to exercise individual rights.

CCPA Compliance: Know Your Data (Continued)

- Technical Approach to Data Mapping
 - Identify all your businesses processes in scope for the CCPA:

- Agile Questionnaires



- Data Lifecycle Visualizations



- Data Inventories

Name*	Hosted Country*	Organization*	Owner	Type	Hosting Type	Hosting Provider
Salesforce	United Kingdom	OneTrust Privacy	Dominic Simms	In-House	External	Microsoft Azure
Workday	France	OneTrust Privacy	Dominic Simms	In-House	External	Microsoft Azure
SAP	France	OneTrust Privacy	Dominic Simms	In-House	On-Premise	Not Applicable
HR Document Warehou...	France	OneTrust Privacy	Unknown	Unknown	Unknown	Not Applicable
Gusto	Germany	OneTrust Privacy	Richard Daniel	Unknown	Unknown	Not Applicable
Sales Document Wareh...	France	OneTrust Privacy	Richard Daniel	Unknown	Unknown	Not Applicable
Teradata	France	OneTrust Privacy	Unknown	Unknown	Unknown	Not Applicable

CCPA Compliance: Know Your Data (Continued)

- Identifying PI Within The Data Environment
 - Methods:
 - Regular expression searching
 - Neural networks and advanced A.I.
 - Human review
- Safeguard against data breach
 - Minimize – purge redundant, obsolete and trivial data
 - Protect – ensure adequate safeguards for sensitive data
 - Review ACLs
 - Restrict access
 - Redact
 - Monitor in place
 - Review access logs
 - Monitor metadata elements indicating breach

CCPA Compliance: Know Your Data (Continued)

- Data Strategy, Transformation and Innovation
 - Begin incorporating privacy by default and by design into your processes.
 - Create a process for evaluating new in-scope data processes to ensure CCPA compliance.
 - Create a process for building compliance into your M&A workflows.

CCPA Compliance: Third Party And Ecosystems

- Key Steps
 - Know your in-scope data flows and identify your business partners.
 - Create proper contractual obligations.

CCPA Compliance: Third Party And Ecosystems (Continued)

- Third Parties vs. Services Providers
 - CCPA makes a distinction between the two
 - To become a service provider, an entity needs to be bound by a written contract that prohibits the entity from:
 - Retaining the PI
 - Using the PI
 - Disclosing the PI
 - Third parties are entities with which a CCPA business with which a CCPA business shares PI and that themselves are neither CCPA businesses, nor bound by a service provider written contract required by the CCPA.

CCPA Compliance: Data Subject Requests -- The Technical Perspective

- Maintaining an inventory of PII
 - Inventory of all locations containing PII
 - Search capabilities across these locations
- Documented process to gather, redact and purge data
 - Know how to gather the documents
 - Plan for review and redaction
 - Ensure verified purging process

CCPA Compliance: Data Protection and Security

- California Attorney General enforcement
 - Businesses have 30 days to cure alleged violations
 - Up to \$7,500 per intentional violation
- Data breach private right of action
 - Loss, theft, unauthorized disclosure of certain types of non-encrypted or non-redacted PI due to failure to implement and maintain reasonable security procedures.
 - Types include: SSN, account numbers (and passcodes) and medical PI
 - Actual or statutory damages → \$100 - \$750 per incident
- Possible expansion?
 - Consumer groups advocating for expanded right of private action → seeking right to sue for all violations under CCPA.
 - Again, know your data!
 - Understanding data assets key to rapidly respond to data breach and remediate as necessary.

What's Next?



:

Key first decisions setting new standards, precedent and clarifying ambiguity

Notable sanctions/penalties

Additional States and/or Federal Following Path Paved by CCPA