



5 Best Practices for Compliance with the CCPA

October 23, 2020

Buchanan
Ingersoll • Rooney

ACC Association of
Corporate Counsel
— NATIONAL CAPITAL REGION —

Panel



Amy Miller
Buchanan Ingersoll & Rooney
Shareholder
202-452-7935
Amy.miller@bipc.com



Jason Parish
Buchanan Ingersoll & Rooney
Shareholder
202-452-7940
Jason.parish@bipc.com



Sue Friedberg
Buchanan Ingersoll & Rooney
Shareholder
412-562-8436
sue.friedberg@bipc.com



Veronica Torres
Comscore, Inc.
Chief Privacy Officer
707-234-2606
Vtorres@comscore.com



Jennifer Mailander
Fannie Mae
Deputy General Counsel
202-752-4667
jennifer_mailander@fanniemae.com

Agenda

- What is the CCPA? Overview and Timeline
- What are the Stakes? Private Right of Action & Statutory Damages
- 1. Best Practices for Getting Started
- 2. Best Practices for Handling Personnel PI and Business Contacts
- 3. Best Practices for Preparing for Consumer Exercise of CCPA Rights
- 4. Best Practices for Employee Training
- 5. Best Practices for Responding to CCPA Requests
- Response to Survey Questions

What is the CCPA?

Overview and Timeline

CCPA Protects “Personal Information”

“***Personal information***” (***PI***) is information that:

- Identifies, relates to, describes, is capable of being associated with a particular consumer or household, or
- Can reasonably be linked, directly or indirectly, with a particular consumer or household.
- CCPA identifies 11 distinct categories of PI
- PI does not include “de-identified” or aggregate information

CCPA Protects “Consumers”

Consumers are essentially California residents, i.e. natural persons who:

- Reside in California for other than a “temporary or transitory purpose,” or
- Domiciled in California, but outside of the state for a “temporary or transitory purpose.”
- “Consumers” include employees and personnel of a Business, as well as business contacts (but many CCPA requirements deferred until 2022 for PI of these groups, pending alternative legislation)

New rights for “consumers”:

- **Know** what PI is being collected, disclosed, and sold, and to whom;
- **Access** to PI (portable form);
- **Opt out** of the sale of PI;
- **Deletion** of PI, unless one of the CCPA’s broad exceptions apply; and
- **Nondiscrimination** in service and price for consumers who exercise privacy rights.

Personal Information: 11 Categories

1. **Identifiers**: 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.
2. **Associated with a consumer**: signature, physical characteristics, telephone number, state identification card number, insurance policy number, education, bank account number, credit card number, debit card number, medical information, or health insurance information.
3. **Characteristics of protected class** : gender, race, religion, ethnic origin
4. **Commercial** : records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
5. **Biometric data**

More PI Categories

- 6. **Internet or other electronic network activity** : browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
- 7. **Geolocation**
- 8. **Sensory**: Audio, electronic, visual, thermal, olfactory, or similar information
- 9. **Professional or employment-related**
- 10. **Education** information that is not publicly available; **AND...**
- 11. **Inferences** drawn from any of the other types of personal information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Who Must Comply with the CCPA?

1. Any business (Business):

- For-profit
- “Doing business” in CA;
- Collects PI about consumers; and
- Meets any one of these criteria:
 - Annual gross revenues worldwide > \$25 million
 - 50% or more of gross revenues derived from selling PI, **OR**
 - Annually receives or buys PI of 50,000 consumers, households, or devices
- Includes parent and affiliated companies that have common branding with the Business

Who Must Comply with the CCPA?

2. “Service Providers”

- For-profit entities
- Must process PI only for a necessary “business purpose” on behalf of a Business
- Must agree in a written contract with the Business:
 - To use the PI only for the specific contract purpose
 - Not to use, sell, retain, disclose, or further collect the PI for its own commercial purposes
 - To comply with these restrictions
- Liable under CCPA for violating the written contract obligations
- Required to delete PI when directed to do so by the Business
- Business is not liable if its Service Provider violates the contract (unless Business had reason to believe the Service Provider intended to violate)

Who Must Comply with the CCPA?

3. “Third Parties”

- **IMPORTANT:** disclosing/selling PI to a third party is major focus of CCPA
- Any individual, company, organization, or group that receives PI, **but is:**
 - Not the Business that collected or is responsible for collecting the PI;
 - Not a parent or affiliate of the Business that uses common branding with the Business; or
 - Not a “service provider”—not prohibited by agreement from selling or otherwise using the PI for its own “commercial purposes”; and
- Presumably “third party” is the buyer or other recipient of PI for its own commercial purposes
- Prohibited from re-selling PI without first complying with the CCPA (i.e. giving required notices and rights to consumers)

Timeline of Key Dates

- **January 3, 2018** – CCPA Introduced
- **June 28, 2018** – Signed into law
- **September 25, 2019 to October 11, 2019** – Governor signs nine amendments, modifying various parts of the law
- **January 1, 2020** – Compliance goes into effect. Covered entities have six months before enforcement begins, although actions taken (or not taken) after this date could be subject to enforcement after July 1, 2020.
- **February 3, 2020** – The first legal complaint citing the CCPA, *Barnes v. Hannah Andersson*, is filed in the Northern District of California. Plaintiffs sue retailer Hanna Andersson and Salesforce.com over a data breach suffered by Hanna Andersson, citing the CCPA
- **February 10, 2020** – The California Attorney General's Office issues its first set of modifications to the proposed enforcement regulations
- **March 11, 2020** – The California Attorney General issues its second set of proposed modifications—modifying various definitions and removing previous requirements like the controversial opt-out icon
- **July 1, 2020** – Enforcement of the CCPA begins despite concerns about COVID impacting the ability of businesses to conform practices to the new regulations
- **August 14, 2020** – Final Regulations approved; effective immediately
- **October 12, 2020** – Modifications to CCPA regulations proposed by Attorney General's office
- **November 3, 2020** – Californians vote on the "California Privacy Rights and Enforcement Act of 2020" (CPRA) which would substantially alter CCPA



Do Not Sell My Personal Information

What are the Stakes?

Private Right of Action & Statutory Damages

What are the Stakes?

- ***CCPA Private right of action only for breach of duty to maintain “reasonable security” measures to protect sensitive PI***
 - 30-day pre-suit notice and opportunity to cure (if curable)
 - Statutory damages = greater of \$100-\$750 “per consumer per incident” or actual damages
 - Class action
- ***No private right of action for violations of privacy rights (e.g. disclosure requirements, “Do Not Sell” option, etc.)***
- ***California AG can enforce any CCPA violation***
 - Business gets 30-day cure period for “any alleged violation” under the CCPA
 - Civil penalties reaching \$2,500 per violation or up to \$7,500 per intentional violation
 - Delayed until July 1, 2020

But, complaints filed since CCPA effective date also allege other claims & statutory damages for privacy violations:

- Breach of CA Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200 to 172010):
 - Statutory damages
 - Permits class actions
 - Requires 30 day notice/cure period
- Common law negligence
- Breach of contract
- Unjust enrichment

#1 Best Practices for Getting Started

Business-to-Consumer Issues

1. Undertake data mapping—in depth study of all PI collected, what purpose, where is it located, who has access to it
2. Identify all points of collection of PI—online and offline
3. Determine if you are “selling” PI (including exchanges for non-monetary consideration)
4. If you are selling PI, consider whether you need to meet the disclosure and non-discrimination requirements for financial incentives
5. Update Privacy Policy (required annually)
6. Ensure website compliance for accessibility, required links to Privacy Policy, Notice at Collection, opt-out form for “Do Not Sell MY PI” if applicable, and webform for consumers to exercise their CCPA rights
7. Train employees in CCPA requirements and how to respond to consumer requests
8. Locate, review, and amend contracts with Service Providers and Third Parties to cover CCPA requirements and issues

Business-to-Business Issues

- 1.** Does your B2B service involve access to consumer PI (the customers of your customer)?
- 2.** Are you subject to contractual obligations to protect your customers' PI?
- 3.** What contractual security obligations can you reasonably comply with?
- 4.** Are you prepared to provide breach notification to your customers?
- 5.** Should you have a Privacy Policy for data collected:
 - Website analytics
 - Digital marketing?
 - How you process your customers' PI?

Website Accessibility

Implement reasonable accessibility standards –

- The CCPA requires that consumer facing privacy disclosures, notices and policies be accessible to individuals with disabilities
- A Business's method for consumers to make CCPA requests should be tailored to enable requests by all consumers, regardless of disability, or specific alternatives should be made available to individuals with disabilities
- The CCPA Regulations specifically reference the Web Content Accessibility Guidelines (WCAG), version 2.1, as among the “generally recognized industry standards” that businesses should use to enable access

Documenting Compliance through Record Retention

- **Record retention is required:** A Business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at **least 24 months**. The Business shall implement and maintain reasonable security procedures and practices in maintaining these records.
- If a Business sells or shares more than 10,000,000 consumers' personal information in each calendar year, additional record keeping is required.
999.317(g)

#2 Best Practices for Handling Personnel PI and Business Contacts

Best Practices for Personnel PI

How should a Business handle employee data and does the manner of handling that data change if the Business has employees in multiple states?

- CCPA treats the PI of all personnel of a Business (“Personnel”) the same way
- Treatment applies to current and former employees, contractors, directors, officers, controlling owners, their emergency contacts, beneficiaries of plans, and job applicants

Best Practices for Personnel PI

PI used solely for personnel-related purposes is exempt from CCPA until January 1, 2022

- Exception—must provide notice of personal information collected and the purposes of collection
- Exception—private right of action for failure to use reasonable security measures and a breach occurs
- January 1, 2022, Personnel will have the same rights as all other consumers (i.e., right to know, right to access, right to opt out, and right to deletion)
- Be alert for possible changes in the CCPA or new laws covering Personnel

Best Practices for Personnel PI

- Prepare a Personnel-specific privacy notice and distribute to all California Personnel (including applicants)
- Review HR data systems (e.g., data mapping) to determine Personnel PI is stored, to enable responses to requests effective January 1, 2022
- Determine if any Personnel PI is “sold” to third parties (e.g. sale of customer or lead lists); if so, implement opt-out process from sales to third parties
- Implement Service Provider contractual obligations from Third Parties with access to PI of Personnel and business contacts

What About Business Contact Information?

- PI of your business contacts is exempt from CCPA requirements until January 1, 2022 IF used for B2B transactions or for due diligence
 - Exception—if information is “sold” to third party, the individual must be offered the right to “opt-out” of sale
 - Exception—private right of action for failure to use reasonable security measures and a breach occurs
- Examples: PI of business contacts includes name, employer, position, contact information

#3 Best Practices for Preparing for Consumer Exercise of CCPA Rights

Do You Have the Right Methods for Consumers to Submit CCPA Requests?

- Businesses must designate at least two methods to submit a request
 - An email address, website form, or hard copy form.
- Must be a toll-free phone number
- If the Business has a website, one of those methods has to be through its website
- If a Business operates exclusively online, and has a direct relationship with the consumer, it only needs to provide an email address for submitting requests to know

Sony.com Access My Personal Information Request for California Residents

Submit Your Request


Please complete the following fields to make your access request which is limited to name and email address, that you provided to Sony.com for newsletter subscriptions.

All Fields Are Required

I request access to the categories of personal information ▼

Please validate below captcha.

☐ I'm not a robot


reCAPTCHA
Privacy · Terms

By clicking the 'Submit' button, you are declaring you are a California resident and authorized to make this request.

Does Your Business Have the Right Procedures for “Do Not Sell My Personal Information”?

- **Opt-Out Requests:** Businesses that “sell” PI must permit Consumers to “opt out” of such sale. Requests to Opt-Out should be handled through same method as Requests to Delete and Requests to Know.
 - A clear and conspicuous link titled “Do Not Sell My Personal Information” must be posted on your homepage. This link must enable a consumer, or person authorized by the consumer, to opt out of the sale of the consumer’s personal information, even if they do not have an account. To be safe, companies may want to post notices directly above all website submission fields, rather than at the bottom of the page or embedded in a footer.
 - For offline collection: at the very least, privacy policy URL should be provided at point of collection.
- **What is a Sale?** Under the CCPA, “sales” include any transfer of PI to a third party, other than to a service provider, for value. This includes both exchanges for monetary compensation **and** non-monetary compensation (e.g., Business sends PI to a third party and receives a detailed analysis regarding the PI, and the third party keeps the PI as payment for the analysis).

#4 Best Practices for Employee Training

Are Your Employees Trained to Handle Consumer Requests?

- **CCPA requires appropriate employee training:** All individuals responsible for handling consumer inquiries about the Business's privacy practices or the Business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.
- Establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the Business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.



Best Practices Employee Training

■ Practical Pointers

- Create a training policy and incorporate into your organization's training schedules for other laws such as consumer financial protections, HIPAA, cybersecurity, etc.
- Train all personnel on the basics of CCPA, including consumer rights, how consumers can make CCPA requests to your organization and where to direct consumers who want more information about their rights (i.e., your organization's Privacy Policy and privacy officer)
- Identify any personnel who actually collect PI directly from consumers or who will be present at point of collection (e.g., customer service representatives, marketers, and others, as well as often overlooked individuals such as call center and online chat personnel, store clerks, independent contractors, etc.) and **ensure "notice at collection" process is clear and well-understood**
- If a large volume of requests are received or anticipated, establish and train dedicated team who will process CCPA requests and provide more rigorous trainings to such personnel. Consider deploying an automated request processing and tracking service.

#5 Best Practices for Responding to CCPA Requests

Responding to CCPA Requests

- **Right to Know Request:** Business must provide the following information *without charge* related to the 12 months preceding the Request, as it relates to the specific consumer:
 - The **categories** of personal information collected
 - **Specific pieces** of personal information collected (but not the actual identifier)
 - The categories of **sources** from which the Business collected personal information
 - The **purposes** for which the Business used the personal information
 - The categories of **third parties** with whom the Business **shared** the personal information
 - The categories of information that the Business **sold or disclosed** to third parties

Responding to CCPA Requests

- **Right to Delete Request:** Business must locate and delete PI it has, and direct Service Providers to delete, unless an exception applies, unless the PI:
 - **complete the transaction** for which that personal information was collected, to provide goods/service requested by the consumer or that may be requested given the nature of the business relationship, or to otherwise perform its obligations under a contract with the consumer;
 - **detect security incidents or debug systems** and protect against malicious, fraudulent, or illegal activity;
 - **exercise free speech** or another right provided by law;
 - **comply with legal obligations;** (must tell consumer why if Business is denying request)
 - **engage in peer-reviewed research;** or
 - **enable internal uses** that are “reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the Business,” and to otherwise use internally, the personal information in a lawful manner that is “compatible with the context in which the consumer provided the information.”

Responding to CCPA Requests

- **Practical Pointers**

- 1) Businesses cannot require a consumer to create an account just to submit a request to know, but if a consumer already has an account with the Business, it may require the consumer to submit the request through that account
- 2) Businesses must acknowledge receipt of a request within 10 business days and substantively respond to requests within 45 calendar days. They can extend that deadline by another 45 days (90 days total) if they provide notification including telling the consumer the reason for the delay
- 3) Businesses must verify that the person making a request to know is the consumer about whom the Business has personal information. Businesses may need to ask for additional information for verification purposes. If the Business asks for personal information to verify identity, it can only use that information for this verification purpose

Is your verification process tailored to your Business's data collection?

- Verification is not required for opt-out, but additional information may be required to confirm the correct person's information is not being sold
- Verification required for Right to Know and Right to Delete requests. Verification should be tailored to the type of PI the Business has and the potential harm to the consumer if a malicious actor were to successfully make a request on his/her behalf
 - Consider the type of information that will be disclosed and whether such information's disclosure could harm the consumer. Sensitive information (SSN, Driver's License, credit card numbers) should never be disclosed.
 - Consider the effect on the consumer of the request. For example, improper deletion of a consumer's Instagram or Facebook would likely be more harmful than improper deletion of a consumer's email address from a marketing website.

Common Identity Verification Techniques

- Basic requests for non-sensitive information can be validated with a code sent to a consumer's phone or email address on file
- Consumers should be able to provide basic information about their interactions with you, such as user ID, answers to security questions, order numbers, etc
- Usage of an existing account can authenticate users for basic/non-sensitive requests or for requests with a low risk of harm to the user
- For more sensitive / potentially harmful requests, consider using third-party organizations that can verify individual's identity, such as Experian
- If necessary, request copy of photo ID

What if a consumer makes a request without following your designated process?

- If an individual makes a request (or an arguable request) under the CCPA without using the designated request method, the Business may either:
 - treat the request as if it has been made using the designated request method and respond accordingly; or
 - direct the consumer to the Business's designated manner of making CCPA requests.
- Recommendation: Direct consumers to use the designated method for making CCPA requests, unless the consumer is unable to use the designated method (e.g., if the consumer has a disability preventing their use of such method). Include this in employee training.
- Designated process for submitting and responding to requests facilitates: tracking requests and response deadline; generating consistent responses, verifying the requestor's identity, verifying the requestor's authority to make request (on their own behalf or behalf of another), and escalating for legal/compliance review when appropriate.

What if a non-resident of CA makes a CCPA request?

- This should be a business decision made upfront—whether to treat everyone the same or limit CCPA rights to CA residents only
- Generally suggest limiting these rights to CA residents only by making that clear in the Privacy Policy and website forms
- May want to offer access to PI collected, but not deletion and “Do Not Sell” rights
- Review the state of residence of the requestor to be sure there are no state requirements (e.g. Nevada has some similar requirements; many states require access by employees to their employment records)
- Prepare a template response letter for non-CA residents explaining that the action requested is not legally required (perhaps offer an alternative)

Response to Survey Questions

How should a Business handle offline (e.g., in-person) collection of data?

- CCPA applies regardless of how the Business collects the information
- Businesses must provide notice that it is collecting personal information at or before the point at which the Business collects personal information.
 - Collection points can include **active** collection (e.g., soliciting using a web form) and **passive** collection (e.g., through data analytics through website)
- Privacy Policy must describe the Business's practices, **both online and offline**, regarding the collection, use, disclosure, and sale of personal information, and of the rights of consumers regarding their own personal information.

Practical Tips for Offline Data Collection

- CCPA Regulations Section 999.305(3)(c): “When a Business collects consumers’ personal information offline, it may include the notice on printed forms that collect personal information provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.”
- Businesses that operate storefronts and collect data offline should have available printed CCPA request forms, privacy policies, and notices at the point of collection; train employees who collect personal information; and post conspicuous signage, including “Do Not Sell My Personal Information” notices within their stores.
- Business that substantially interact with consumers offline **are not required** to provide a notice to the consumer by an offline method

How to handle sharing/selling with third parties?

- Need to decide if the data sharing arrangement is a “sale” (i.e., if your company is receiving value for the transfer). Sale will trigger the opt-out right and required Privacy Policy disclosures.
- A Third Party who receives PI and intends to use the PI for its own purposes will have the same obligations to consumers as any other Business covered by the CCPA. Third parties who purchase or receive PI from a Business, but do not directly collect the PI from consumers, are not required to provide a “notice at collection” to the consumers, unless they intend to re-sell the PI.
 - Example: a Third Party performing market research may purchase PI from a Business and use it internally without providing a “notice at collection”. But, if the Third Party intends to further sell the data to other companies, it must provide the notice and the opportunity for the consumer to opt-out of the sale.

How do Service Providers (CCPA) and Processors (GDPR) compare?

How does the concept of independent data controllers (to take the GDPR term) apply under the CCPA? For example, how does California view that analysis, if service providers collect additional personal information from data subjects not dictated by and supplied to the Business are they only a Service Provider or are they both a Service Provider and a Business?

A company can be both a Service Provider and Business

- CCPA: a Service Provider is the agent of the Business (principal)
- GDPR: a Processor is the agent of the Controller (principal)
- If the Service Provider/Processor collects further PI or otherwise operates outside the scope of its agreement with the Business/Controller, it must comply with the requirements for a Business/Controller with respect to its out-of-scope activities
- Examples:
 - Service Provider is a Business with respect to its own Personnel's PI
 - Service Provider may have both B2B (as Service Provider) and B2C (as Business) operations
 - Parties may have a data sharing arrangement with elements of both functions

If passed, how will the CPRA change compliance?

The CPRA contains literally hundreds of small and major changes and likely will affect various organizations in very different ways. The CPRA would most notably:

- Prohibit a Business from retaining personal information for longer than “reasonably necessary” for the disclosed purpose
- Create a new California Privacy Protection Agency to enforce the privacy laws with funding of \$5 million dollar for the remainder of the first fiscal year and \$10 million per fiscal year (July 1 to June 30) thereafter
- Permit consumers to opt out of the sale “or sharing” of their data
- Dictate terms for contracts with third party when a Business collects a consumer’s Personal Information and sells or shares that information

Thank you!

Amy Miller
Buchanan Ingersoll & Rooney
Shareholder
202-452-7935
Amy.miller@bipc.com

Jason Parish
Buchanan Ingersoll & Rooney
Shareholder
202-452-7940
Jason.parish@bipc.com

Sue Friedberg
Buchanan Ingersoll & Rooney
Shareholder
412-562-8436
Sue.friedberg@bipc.com

Veronica Torres
Comscore, Inc.
Chief Privacy Officer
707-234-2606
vtorres@comscore.com

Jennifer Mailander
Fannie Mae
Deputy General Counsel
202-752-4667
Jennifer_mailander@fanniemae.com