GRAYHAIR

Understanding CCPA Requirements, Privacy & Postal Data

The California Consumer Protection Act (CCPA) is a comprehensive privacy regulation that defines privacy rights and protections for California consumers. It is the most recent personal data protection law passed by the State of California as a response to the increased role of personal data in contemporary business practices and the personal privacy implications surrounding the collection, use, protection, and sale of personal information. It applies to for-profit organizations that collect, process or store personal information pertaining to California residents regardless of where the organizations are incorporated.

Overview of CCPA Regulations

There is a new law in California taking the lead, commonly known as CCPA, that deals in the areas of marketing, advertising, and data.

The CCPA puts limits on the transfer, the disclosure, and the sale of information. Most importantly, it also creates a prior right-of-action under the law related to the area of security.

The other rights and operative requirements under the CCPA are enforced by the attorney general. You might be wondering how that enforcement will play out in the market. Anytime you talk about the CCPA, you really have to start off with the unique nature of how this became law.

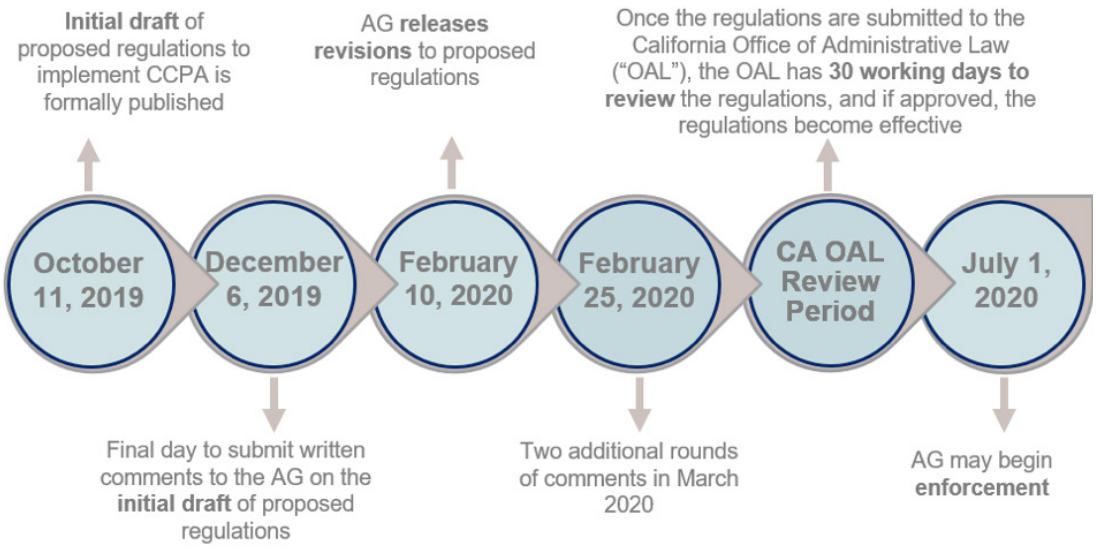
Why the CCPA Matters

- Shift towards the European approach to privacy (GDPR)
- Implementation of consumer-directed disclosures and controls
- Creation of systems and processes to respond to customers
- Navigation of overlapping federal laws
- Extensive potential liability for security breaches

CCPA Regulatory Timeline

In 2017, a wealthy real estate developer, named Alastair MacTaggart, strived to have a ballot initiative submitted for vote by the citizenry of California to enact privacy legislation law. Meaning, it wouldn't go through "regular order of the legislature."

By going through a ballot initiative, it created some unique procedural operative requirements under the law. Now, in particular, the law couldn't be amended except by a super majority of the legislature. Really, what was passed by a ballot initiative would become the law and it would be unlikely that it could change unless it becomes more onerous in nature and also included that super majority. However, there was great concern as this moved through and worked with MacTaggart and the legislature.



In 2018, it moved from a ballot initiative through the legislature and quickly moved through both the Senate and the Assembly, where it was passed. It went before the Governor all within about a seven to an eight-day period, becoming law and signed by at the time Governor Brown. Once it became a law, it went through an amendment process in the fall of 2018 and then in 2019.

Throughout 2019, Governor Brown held a series of public hearings that then commenced in the issuing of a first proposed regulation in October of 2019 with comments being filed by interested parties in December and then a first modification issued in February. Those were due in the first week or so of March. Then, a second modification was released. Those comments on that modification were due on March 27th, 2020. There could potentially be a third modification or move right to final regulations.

> "We're getting quite close to the enforcement date and need to give companies an opportunity to make changes to their operations."
>
> *Michael Signorelli, Partner, Venable LLP*

If there's another issue of modification, it would go to a 15-day public commentary. That can continue on until the regulations are finalized, which then would go off to the Office of Administrative Law for review and publication. There's a 30-day working period available to the California Office of Administrative Law (OAL) to review the regulations. Once published, they become enforceable. Recently, Governor Newsom issued an executive order granting the OAL an additional 60 days to review all regulations. The enforcement deadline is currently set for July 1st, 2020.

On March 20th, a group of trade associations and other organizations and companies sent letters to the Attorney General and the Governor. There were more than 65 signatories requesting a delay of enforcement until January of 2021. There appears to be a reason for this. The rules are not yet final.

The Scope of CCPA

The CCPA applies to a business that has an annual growth revenue over $25 million or collects or shares personal information annually from 50,000 consumers, households or devices, or derives at least 50% of annual revenue from the sale of personal information.

Personal information is any identifiable information like name and address or really any data that is reasonably capable of being associated or linked directly or indirectly with a consumer or a household. A consumer means any natural person that is a resident of California, which also, in this case, includes business to business information as well as employee data.

There are three categories of covered entities. We've already covered what a business is, but there's also service providers and third parties. Service providers are entities that work at the direction of a business. They're under contract and the contract prohibits the service provider from using, retaining, or disclosing any of the personal information received in the provision of services except for the business purposes identified in the contract.

If a partner is a service provider, the transfers between the business and the service provider would not constitute a sale, meaning that would not apply there. But it certainly puts in some limitations on how the information can be used, per the regulations promulgated by the attorney general. While they may be able to use it to improve the quality of services, there are limits about building out profiles or modifying data sets that will be used for other clients or customers of the service provider.

The last category is the third party. It's not the business or a service provider but the concept is they're not collecting data directly from the consumer collecting personal information. The types of data that are enumerated in the CCPA are examples of what constitutes personal information as any sort of identifier, so names, postal addresses, and online identifiers, such as cookies or IP addresses could be personal information. Also geolocation information, any sort of behavioral data, so web viewing data, clickstream data could constitute personal information under the law.

There are a few exemptions to personal information. De-identified data, aggregated information, and publicly available information isn't considered personal information under the law.

There are a few key rights that you should be aware of:

1. Access

   Under the law, consumers have the right to gain access to personal information collected about them. That includes the specific pieces of information collected about that consumer, so businesses are expected to provide a mechanism to that consumer where they can make such a request and upon verification of that consumer. Once the request and verification

have been made, a business is expected to return the specific pieces of information that is collected, as well as information about the categories of entities they disclose information to, who they've sold it to, and their sources.

2. Deletion

   Consumers have the right to delete information and it is information collected from the consumer that is subject to this right. There are some exceptions where information is needed for providing the services or certain security exceptions to the rule as well. Mentioned earlier there is an opt-out under the law and it's with respect to the sale of information. It's not opt-out from the collection or uses processing information. It's relevant to understand the contours and the scope of what sale means.

3. Right to Opt-Out

   This includes the selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating personal information by the business to another business or third party for monetary or valuable consideration. It's a rather broad definition. What wouldn't be included here is transfers to a service provider subject to a contract with specific restrictions on the use of the information. But this right is available to the consumers. Companies or businesses implementing this have certain disclosure obligations related to putting the do not sell my personal information link on their website that allows consumers to direct a business not to sell information.

There are statutorily defined deadlines by which you must respond to rights requests for access and deletion, and it'd be best to have those at the ready should those requests come in.

Understanding Privacy and Postal Data

The Postal Service™ maintains a lot of different types of data, including data that is regularly exchanged between the Postal Service, its customers, and mail service providers.

As you might expect, this data primarily consists of names and addresses but there's also other information associated with those names and addresses particularly related to mail delivery, and change of address information. As you may know, the Postal Service maintains the national Change of Address (NCOA®) database, and it licenses access to this database through various products. This database combines name and address information with change of address information that the Postal Service maintains. This change of information comes from change of address forms submitted by postal customers, as well as from information obtained by mail carriers. Under the postal regulations, to be compliant with and eligible for certain discounted rates, mailers need to run their lists through the change of address database and update their list prior to mailing. This is often accomplished by hiring a third party who maintains an NCOA license to provide the service.

The Postal Service also provides the Address Correction Service (ACS™), which is another change of address product, but it's a post-mailing service rather than a pre-mailing service like NCOA. It can provide Undeliverable-As-Addressed (UAA) codes that identify the reason a mailpiece was not delivered to a particular address and that can include codes indicating that the address is invalid or that the customers moved and did not leave a forwarding address.

We know that information is going back and forth between the Postal Service mailers, service providers, and other parties and the question is, **what does that mean under the CCPA**?

What It Means Under the CCPA

The first thing we're going to do is we're going to assume for right now that all these private entities involved in these transactions are businesses under the CCPA. They have 50,000 customers or they have $25 million of gross revenue. If that's the case, the first information we're going to ask is whether the information being traded around is personal information.

The other question to ask is whether the information is publicly available and as my detail that's information that's lawfully made available from government records and importantly, here that information does not need to be directly acquired from a government source.

Public vs. Private Data

NCOA and ACS data is sourced from the Postal Service. The Postal Service is a government entity so this information is for the most part, publicly available information, therefore outside the definition of personal information. We find the same thing with Undeliverable As Addressed codes again, while this information can be associated with individual households, it's coming from the Postal Service.

Where we get into some more difficult questions is maybe when we're talking about the third party information. If you have names and addresses that are coming from customers directly or that have been purchased from list providers, it might be the same information as the information that's being provided by NCOA and ACS, but because it's not coming from a government source, it falls within the definition of public information.

The bottom line for compliance seems to be pretty straightforward, right? The data that's provided by the Postal Service is publicly available information because it's coming from a government source. Companies that are only collecting and using this publicly available data are not subject to the CCPA compliance obligations. However, if the same information is being provided by private sources that may be personal information unless the data originally comes from a public source.

> "The important thing to remember here is that publicly available information remains publicly available information even when it's transferred through private parties."
>
> *Matt Field, Partner, Venable LLP*

Again, we have to trace it back to where it's coming from originally and if your companies that are collecting and using this personal information that doesn't come from a public source might have CCPA compliance obligations. That seems pretty straightforward, if it comes from a private source, you have obligations, public source, the obligations, aren't there, right? Well, not so fast. There's one piece to remember and that's the issue of service providers.

The Role of Service Providers

Specifically, there is the issue where a company has information that they've compiled from whatever sources that may be personal information subject to CCPA, and they want to provide that information to a service provider who will then perform change of address services for them using the Postal Service information. While disclosing that information to the service provider could be seen as a sale under the CCPA because as long as that service provider is just processing the personal information on behalf of a business and as contracted prohibits the use or disclosure of that information for purposes outside the contract, they're a service provider.

That takes them out of the realm of the CCPA or at least out of the compliance obligations associated with the sale of information.

Data Security, Postal Regulations & The Future

SOC2 with HITRUST - it is really important to make sure that you have the right data classifications in place. Whether data is considered public, private or confidential, along with HITRUST mapping to make sure that if your data are on the cloud or you have multiple data centers, that you have the right procedures in place for managing data.

PCI Compliance - critical if you're dealing with credit card information. It also includes provisions around verification of information that's being destroyed. It needs to go through a two verification process.

HIPAA - consists of some very strict laws for those dealing with insurance and medical record information.

HR Security Policies - these are your companies data security policies, practices, and rules on what you can and cannot do. Companies should also put in a policy that requires going through annual intrusion detection to test systems and address any vulnerabilities.

Encrypted Data at Rest - when it comes to storing data, are you storing your data in an encrypted form at rest? If someone tries to hack into your system, they will not be able to make any use of encrypted data in your custody.

Worldwide Developments

There are many countries that have taken up privacy legislation of various different kinds. The first one that most people have probably heard of is the GDPR, which covers the European Union and continues to expand. Other countries as well as states around the US are starting to follow suit.

In 2019, there were approximately 20 states that have put forward different privacy legislation. In 2020, we're expecting several additional states to enact new legislation.

USPS Impacts

The Postal Service has remained silent on this issue, leaving the industry to navigate privacy waters on their own. As a result, people might make the decision to store less and less information such as mailing lists to prevent exposure. For example, due to mail volume declines, the catalog industry is having a hard time trying to get mailing lists to mail out catalogs. Part of that is the decline in mail volume within the mailing industry, but part of that is directly related to these new regulations.

We have to be really careful as an industry, how we adhere to the new regulations, and how we move forward, especially with all of these other states trying to introduce legislation. Luckily, US products and services are not currently affected, especially around NCOA and ACS data.

> "There are a lot of changes that need to be made with the CCPA, however, it will create new opportunities, especially for the postal industry."
>
> *Angelo Anagnostopoulos, VP Postal Affairs, GrayHair Software*

Some people are required to retain data, especially for end of the month reconciliation, when you have to prove that you were in compliance with things like USPS scorecards, especially if you fall outside of a threshold. If you're maintaining data, how long are you holding on to that data? What happens if your customer gets a request from somebody in California to be purged from all data that are collected about them? Do you have things in place to purge it out of your data stores?

You will have to go in and put processes in place to be able to either purge old data or have a data archival strategy. These are things that you have to think about regarding some of the USPS programs that are out there.

We think that there are going to be ramifications of these new requirements, especially since you will likely need to get permission in order to be able to collect and use information to create profiles. This starts to take you down a dangerous path if not done correctly. As far as websites, you need to put things in place to allow for opt-out, especially if you're collecting information that's considered private; you have to allow people to opt-out. Websites have to be updated to allow for compliance.

We think that there are going to be ramifications of these new requirements, especially since you will likely need to get permission in order to be able to collect and use information to create profiles. This starts to take you down a dangerous path if not done correctly. As far as websites, you need to put things in place to allow for opt-out, especially if you're collecting information that's considered private; you have to allow people to opt-out. Websites have to be updated to allow for compliance.

If you've noticed lately, pretty much any website that you go to, you have to specifically allow that company to store cookies on your computer, because that's considered private information as well.

You also need to track the usage and access of PII, which means your systems have to have really good logins as far as who's using the information, who has access to the information, do they have the right security clearance to have access to that information, and making sure that party A can access party B's information and that.

If you need help ensuring that your business is in compliance with the CCPA, contact the postal experts at GrayHair Software for more information by calling 866-507-9999 or sending a message to info@grayhairsoftware.com.

About GrayHair Software

GrayHair is the trusted partner and provider of mail tracking and address hygiene services to the largest mailers in the country. Our solutions deliver insights and decision-ready business intelligence that enable our clients to define the best mailing practices, enhance customer engagement, increase response rates, and decrease costs per acquisition. With GrayHair, mailers gain the guidance and confidence of 200+ years of collective postal experience and an ally with an understanding of the postal industry's nuances. GrayHair is the advantage for marketing agencies, mail service providers, and mailers in the finance, insurance, retail, non-profit, and utilities industries. For more information, visit GrayHairSoftware.com.

124 Gaither Drive, Suite 160, Mt. Laurel, NJ 08054-1719
GrayHairSoftware.com | engage@grayhairsoftware.com | 866-507-9999

GRAYHAIR