ERVIN COHEN & JESSUP LLP

BUSINESS GUIDE TO THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018: FIVE STEPS IN PREPARATION FOR COMPLIANCE

Jeffrey R. Glassman, Partner
Ervin Cohen & Jessup LLP

9401 Wilshire Blvd., 9th Floor, Beverly Hills, CA 90212
310.273.6302 | jglassman@ecjlaw.com | www.ecjlaw.com

TABLE OF CONTENTS

INTRODUCTION

In June 2018, California enacted one of the most comprehensive privacy laws in the country, the California Consumer Privacy Act of 2018 (the "CCPA"). Although the CCPA will not go into effect until January 1, 2020, businesses should immediately take steps to determine whether it applies to them and, if so, begin implementing procedures that will enable them to comply with the CCPA once it takes effect. Businesses that fail to timely comply could receive substantial fines. Therefore, if your business collects, stores, shares, transfers or sells personal information of California residents, you will want to take the *five* steps outlined herein.

STEP 1: DETERMINE IF THE CCPA APPLIES TO YOUR BUSINESS

Prong 1:

The CCPA applies to certain *for-profit* legal entities *doing business in California that collect, transfer, or sell personal information of California residents*, and determine the purpose and means of processing such personal information. A company may be physically located outside the State of California and still capable of "doing business in California" if they sell goods or services to California residents. Moreover, personal information is broadly defined under the CCPA to include any information about California residents that is capable of being linked with a particular California resident including, but not limited to, the following:

1) Identifiers (Name, address, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, etc.);
2) Commercial Information (Records of personal property, products or services purchased, or obtained, or other purchasing or consuming histories);
3) Biometric Information (Body measurements including fingerprint, palm print, face recognition, DNA, iris recognition, retina and odor/scent);
4) Internet Information (Browsing history, search history, and information regarding a consumer's interaction with an Internet Website, application, or advertisement);
5) Geolocation Data (Information used to identify a device's physical location);
6) Employment or Education (Information about a consumer's employment or education); *OR*
7) Inferences (Any inferences from any of the information identified to create a profile reflecting consumer's 'preferences, characteristics, psychological trends, behavior, attitudes, intelligence, abilities, and aptitudes).

Prong 2:

In addition to the aforementioned *Prong 1* criteria, a business must also fall into one of the following three categories in order for the CCPA to apply:

1) Your company has annual gross revenues in excess of $25,000,000;
2) Your business derives at least 50% its annual revenue from selling consumer's personal information; ***OR***
3) Your company buys, sells, shares or receives for commercial purposes (i.e. anything that advances your businesses economic interests) the personal information of at least 50,000 consumers, households or devices.

A flowchart for evaluating the applicability of the CCPA to your business is attached hereto as ***Addendum "1."***

STEP 2: KNOW THE RIGHTS OF YOUR CONSUMERS

If your business fits the criteria outlined in both *Prong 1* and *Prong 2* above, then the CCPA applies to you. As a result, you need to understand what rights your consumers have under the CCPA and how such rights may be exercised. The term "consumers" as used throughout this guide shall refer to natural persons who are California residents. Here is a brief overview of some of the primary rights consumers have under the CCPA:

RIGHT TO REQUEST INFORMATION

Consumers have the right to both access any personal information a business has collected about them, and to request that a business delete any such personal information.

1) A consumer has a right to request that your company disclose to him or her both the categories and specific pieces of personal information you collect about them for a "business purpose." Collection of personal information by your company will be considered collection for a "business purpose" if (a) use of such information is for your company's own operational purposes (or those of your service providers), and (b) use of such information is reasonably necessary to achieve such operational purposes.
2) A consumer has the right to request a list of categories of his or her personal information your company sold to a third party within the preceding twelve months. Strangely enough, a consumer also has the right to know if your company has refrained from selling their personal information during that same period of time.
3) A consumer has the right to know the categories of the sources your company uses to collect his or her personal information.
4) A consumer has the right to know what the "business purpose" or "commercial purpose" is for collecting or selling his or her personal information. A "commercial purpose" means information used by you to advance your company's economic interests or induce another party to enter into a commercial transaction with your company.

RIGHT TO OPT-OUT

If you sell consumers' personal information to third parties, a consumer has the right to "opt-out," in which case you may no longer sell their personal information to third parties.

RIGHT OF DELETION (SUBJECT TO EXCEPTIONS)

If a consumer asks you to delete his or her personal information, you must do so unless you qualify for one of the applicable exceptions under the CCPA where it would be deemed necessary for your company (or one of your service providers) to maintain the consumer's personal information despite such request. Here is a brief overview of the applicable exceptions that would enable you to potentially avoid deleting the consumer's personal information despite a request to do so:

1) If you need the personal information in order to complete a transaction with the consumer, provide a good or service requested by the consumer, perform a contract with the consumer, or within the context of the existing business relationship with the consumer.
2) To protect against security threats or to prosecute those responsible for illegal activity.
3) To identify and repair any bugs that impair existing functionality on your information technology network and infrastructure.
4) To ensure other consumers can exercise their right to free speech or any other right provided by the law.
5) To comply with other California and federal privacy laws including the California Electronic Communications Privacy Act. By way of example, if your company is subject to a search warrant issued by a governmental agency for personal information that you have been asked to delete, you will not be required to delete such information despite the consumer's request.
6) For public or peer-reviewed scientific, historical, or statistical research in the public interest as long as (a) it adheres to all other applicable ethics and privacy laws, (b) the deletion of the personal information would negatively impact the research, and (c) the consumer has already provided you with his or her initial consent.
7) For solely internal use by your company that is "reasonably aligned" with the expectations of the consumer based on the consumer's relationship with your business.
8) If your business needs to keep the consumer's personal information in order to comply with other legal obligations.
9) If your business is going to use the consumer's personal information solely for internal purposes.

RIGHT NOT TO BE DISCRIMINATED AGAINST

A consumer has the right not to be discriminated against for exercising his or her rights under the CCPA. To that end, you may not, in response to a consumer exercising their CCPA rights, deny them your goods or services, charge them different prices for your goods or services, provide them with a different level or quality of goods or service, or even suggest to them that will receive a different price for goods or services.

Although your business may not discriminate against a consumer for exercising his or her rights under the CCPA, you may offer a different price and even provide consumers with financial incentives in exchange for such consumer allowing you to make use of their personal information. However, the different price and/or financial incentives must, nonetheless, be reasonably related to the value provided to the consumer by the consumer's data. If financial incentives are available, you must inform consumers of such financial incentives. Furthermore, you may enter a consumer into a financial incentive program only if the consumer opts-in; and even if the consumer does opt-in, he or she may revoke their consent at any time.

STEP 3: DETERMINE THE SCOPE OF YOUR COMPANY'S OBLIGATION

Once you understand the rights of your consumers under the CCPA, you may then begin the process of evaluating the scope of your obligations to such consumers.

OBLIGATION TO INFORM CONSUMERS

If your company collects consumers' personal information, then you must (a) inform your consumers about their rights under the CCPA, (b) disclose the categories of personal information you are collecting, and (c) disclose your purpose for collecting such personal information. This information and these disclosures must be made to your consumers at the point of collection. Moreover, you are prohibited from collecting additional categories of personal information or using personal information for purposes other than those originally stated and disclosed to your consumers without first notifying them.

MEANS OF COMMUNICATION

Your business must provide two or more ways for consumers to be able to submit a request related to his or her personal information. At a minimum, one of these communication vehicles must include a toll-free phone number. You may also provide communication tools through your company's web site and a corresponding website address.

EDUCATE EMPLOYEES

You must educate any and all of your employees who will be responsible for fielding and handling requests from consumers of consumer rights and your company's obligations under the CCPA. Such employees must also understand how to direct your consumers and assist them in exercising their rights under the CCPA.

PRIVACY POLICY

At least once every twelve months, your business must update its online privacy policy. At a minimum, your privacy policy must include a description of consumers' rights under the CCPA, provide consumers with one or more ways to submit requests to your company in exercising such rights, and, if your company sells consumers' personal information, a "*Do Not Sell My Personal Information*" link in the privacy policy itself. If you sell consumers' information to third parties, your privacy policy must inform consumers that they have the right, at any time, to direct your company not to sell their personal information. This is known as the right to "opt out."

Your privacy policy must also state that your business is prohibited from selling a consumer's personal information if you have knowledge that such consumer is less than sixteen years of age. In the case of consumers between thirteen and sixteen years of age, they must affirmatively authorize you to sell their personal information before you can sell their information. If the consumer is less than thirteen years of age, that consumers parent or guardian must affirmatively authorize your company to sell their personal information. These rights are known as the right to "opt in."

NO MANDATORY ACCOUNTS

Your company may not require that consumers create an account before allowing them to exercise their rights under the CCPA. Moreover, you must provide consumers with a list of categories that describe the kind of personal information you have collected about them over the past twelve months. You must also disclose whether that information was sold or not sold over the past twelve months, and whether or not your company may sell a consumer's personal information at all.

SERVICE PROVIDERS

Service providers are those businesses that work in tandem with yours, receive personal information belonging to your consumers, and then process that data pursuant to a contract with your business. If you receive a verified request to delete such information from a consumer, you are required to tell your service providers to delete any personal information belonging to that consumer. Furthermore, you are required to contractually prohibit your service providers from retaining, using, or disclosing the personal information of your consumers for any purpose other than to meet the terms of your contract with such service provider.

THIRD PARTIES

Unlike service providers, third parties are businesses that may use personal information of your consumers for their own means and purposes. Before selling personal information to a third party, you must notify the consumer and provide them with the option to "opt-out" of such sale or disclosure, or the option to "opt-in" in the case of a consumer less than sixteen years of age. Moreover, a third party cannot sell personal information of your consumers which they purchased from your business unless they too give your consumers yet another opportunity to "opt out" (or "opt-in," as the case may be) of such sale. Your consumers can only "opt out" of (or "opt-in" to) the transfer of their personal information to third parties, not to your service providers.

VERIFICATION AND RESPONSE TO CONSUMER REQUESTS

If you receive a request from one of your consumers, the first thing you need to do is verify their identity. You will need to associate the information provided by the consumer in the request with any previously collected personal information from that consumer. Once a consumer's identity is verified, you must promptly take steps to respond to their request. If the consumer requests disclosure and delivery of the information outlined in the CCPA, then you must disclose and deliver such information free of charge to the consumer within 45 days; provided, however, that you are permitted to either charge a fee or refuse to process a request if the requests are "*manifestly unfounded or excessive, particularly because of their repetitive character*." Currently, you are not required to disclose personal information to a consumer more than twice in a twelve month period.

The disclosure from you to the consumer must cover the twelve month period immediately preceding the request including the specific pieces of personal information collected and the categories of personal information collected. In this disclosure, you should also include any personal information collected in order to verify a consumer's identity. There are two ways you can deliver this information to a consumer: (1) In writing through the consumer's account with your business; or (2) By mail or electronically. If you deliver this information electronically, the information should be portable and delivered in a format that allows the consumer to easily share the information with others.

If a consumer asks to have their personal information deleted, then, once again after verification, you must delete the consumer's personal information from your records. In addition, you must instruct any service providers in possession of that consumer's personal information to delete such data from their records as well.

If a consumer "opts-out" of you selling their personal information to a third party, you may not sell such consumer's personal information unless and until that consumer provides you with explicit reauthorization to do so. Moreover, you must wait at least twelve months before requesting such reauthorization.

STEP 4: UNDERSTAND YOUR POTENTIAL LIABILITY

ACTIONS BY THE ATTORNEY GENERAL – VIOLATIONS OF CCPA

The fines for violating the CCPA are one of the many reasons to jumpstart your compliance program. The California Attorney General is authorized to bring an action against you for violating the CCPA. If you violate the CCPA, your business could be fined up to $2,500 for each unintentional violation and up to $7,500 for each intentional violation.

ACTIONS BY CONSUMERS – DATA BREACHES

Consumers have a private right of action to sue your business in cases where there is unauthorized "exfiltration, theft, or disclosure" of their personal information that is a direct result of your failure to "maintain reasonable security procedures and practices."

Consumers can also bring lawsuits for any breach involving their "non-encrypted or non-redacted personal information." Failure to adequately encrypt and redact personal information of consumers that is compromised in a breach, will result in damages against your business of between $100 and $750 per consumer per incident. Consumers may also seek actual damages, injunctive or declaratory relief, and any other relief the court deems proper. In assessing a damages award, judges may consider your company's "assets, liabilities, and net worth."

EXCEPTIONS

The CCPA does not restrict your company's ability to do any of the following:

1) Comply with federal, state, or local laws;
2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;
3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law;
4) Exercise or defend legal claims;
5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the form of aggregate consumer information ("Aggregate consumer information" means information that relates to any categories or groups of consumers where the consumers identities have been removed and is not linked or reasonably linkable to a consumer or household); or
6) Collect or sell a consumer's personal information if every aspect of that commercial transaction takes place completely outside of California.

Moreover, the CCPA does not apply to any of the following:

1) Non-profits
2) Medical information governed by the Confidentiality of Medical Information Act
3) A provider of health care governed by the Confidentiality of Medical Information Act and the Health Insurance Portability and Accountability Act ("HIPPA")
4) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects
5) Sale of personal information to or from a consumer reporting agency under the Fair Credit Reporting Act
6) Financial institutions that are complying with the federal Gramm-Leach-Bliley Act
7) Driver's Privacy Protection Act of 1994

STEP 5: YOUR FIRST NEXT STEPS

CREATE A DATA MAP

You need to audit your personal information collection, storage, and sharing practices. As part of this audit, you should create a detailed data map memorializing in writing where all of your consumers' personal information resides. The audit should leave you with a detailed roadmap and a clear understanding of how to access and potentially delete such information when the time comes. Here are some questions to consider when developing the framework for your audit:

1) What categories and specific pieces of personal information does your business collect from consumers?
2) Do you know the sources of the personal information?
3) Can you identify where and how the personal information is stored?
4) What do you do with the personal information you collect?
5) How long do you keep the personal information and why?
6) Do you have the ability to easily access such information and potentially deliver it to a verified consumer asking for a copy of it?
7) Do you have the ability to delete such information?
8) Is all of the personal information you collect digital? If so, does it reside on your information technology network or does another entity have control over it?
9) If personal information you collect is not digital, where is it located?
10) Do you share personal information with service providers or third parties? If so, how would they answer each of the questions listed herein above?

CREATE ORGANIZATIONAL AWARENESS OF CONSUMERS RIGHTS

As described herein above, the CCPA grants very specific and relatively broad rights to consumers regarding access to and deletion of their personal information. You will need to implement organization-wide protocols and train your employees accordingly in order to ensure that you do not inadvertently violate these rights. Along these lines, you should develop a detailed protocol and a predictable, consistent, reliable process for both verifying consumer identities and responding to consumers' requests. These protocols should be documented and updated from time to time.

In addition, make sure that all of your employees responsible for CCPA compliance develop a deep understanding of your CCPA protocols and processes so they can easily navigate them once consumer requests for access to, or deletion of, information begins. These same employees should also be adept at using the data map you create so that responses to requests are complete, accurate, and timely.

You should also discuss these objectives with your IT professionals and determine whether existing IT infrastructure is even capable of handling your new CCPA protocols. If technology upgrades are necessary, you should make them.

DATA SECURITY AND GAP ANALYSIS

The CCPA mandates that you have "reasonable security measures" in place. The reasonableness of such measures ultimately depends on the type of personal information you collect. Are the data security measures you've taken adequate? Maintaining high levels of security means more than merely preventing unauthorized access to consumers' personal information. You should also asses any latent threats and vulnerabilities to data breaches, rank vulnerabilities, and then address the tier-one red flag security gaps first. You should also evaluate whether more sophisticated data security measures are necessary in light of the kinds of personal information you collect.

The Center for Internet Security (CIS), a community of IT experts, publishes best practices lists for helping businesses mitigae cyberattacks. According to CIS, there are at least five critical tenets of an effective cybersecurity system:

1) Learn from attacks that compromise your systems, and build foundational knowledge based on your businesses real world experience in order to improve your defense mechanisms over time.
2) Prioritize finding solutions for the most dangerous risks that your business faces; then work your way towards resolving the less dangerous risks.
3) Create a common data security language and develop a uniform set of metrics and analytics so that your employees and service providers can communicate more effectively and more accurately measure the success of your data security program.

4) Execute multiple, periodic, recurring data security penetration tests to evaluate effectiveness of your data security system from time to time.

5) Implement automatic, programmed responses to vulnerability, threats and breaches in order to better achieve reliability and consistency in creating a meaningful data security system.

UPDATE YOUR WEBSITE AND PRIVACY POLICY

You should review and revise your online privacy policy to disclose to consumers the scope of personal information you are collecting, sharing, and selling. You also need to inform consumers about the rights they have to access and delete such information. In addition, you should include at least two separate methods for consumers to use when communicating with your business including a website and 1-800 toll free phone number. Moreover, if you sell personal information, you also need a "*Do Not Sell My Personal Information*" button on your website. Privacy policies should also include the appropriate "opt-in" process for obtaining and verifying consent from consumers under the age of 16.

REVIEW YOUR CONTRACTS

You should update any contracts with service providers and third parties with whom you have shared, provided access to, or sold consumers' personal information. Amendments to such contracts should require that service providers and third parties also comply with the CCPA and allocate liability accordingly. The contracts should also ensure that you receive notice of any data breaches involving your service providers and third parties.

You should also reassess your insurance coverage to ensure that your cyber insurance policies adequately insure against new liabilities under the CCPA, if possible.

DISCLAIMER

THIS GUIDE IS BEING PROVIDED FOR INFORMATIONAL PURPOSES ONLY. IT DOES NOT CONSTITUTE LEGAL OR PROFESSIONAL ADVICE.

THIS GUIDE IS NOT A SUBSTITUTE FOR A THOROUGH EXAMINATION OF THE CCPA AND EVALUATING HOW IT SPECIFICALLY APPLIES TO AND IMPACTS YOUR BUSINESS.

THIS GUIDE DOES NOT PROVIDE A COMPLETE ANALYSIS OF THE REQUIREMENTS OF THE CCPA REGULATIONS AS THEY MAY APPLY TO YOUR BUSINESS.

THE CALIFORNIA ATTORNEY GENERAL MAY IMPLEMENT REGULATIONS THAT COULD IMPACT THE CCPA.

THE CALIFORNIA LEGISLATURE MAY AMEND THE CCPA.

THE FEDERAL GOVERNMENT COULD PASS LEGISLATION THAT PREEMPTS THE CCPA.

ACKNOWLEDGMENT

THE AUTHOR WOULD LIKE TO GRATEFULLY ACKNOWLEDGE THE ASSISTANCE OF AVIA COHEN IN CREATING THIS CCPA BUSINESS GUIDE.

ADDENDUM "1"

CCPA FLOWCHART

ERVIN COHEN & JESSUP LLP

Do you collect any of the following personal information from California residents?

Identifiers	Commercial Information	Biometric Information	Internet Information	Geolocation Data	Employment or Education	Inferences
Name, address, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, etc.	Records of personal property, products or services purchased, or obtained, or other purchasing or consuming histories.	Body measurements including fingerprint, palm print, face recognition, DNA, etc.	Browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.	Information used to identify a device's physical location.	Information about a consumer's employment or education.	Inferences reflecting consumer's "preferences, characteristics, psychological trends, behavior, attitudes, intelligence, abilities, and aptitudes."

YES

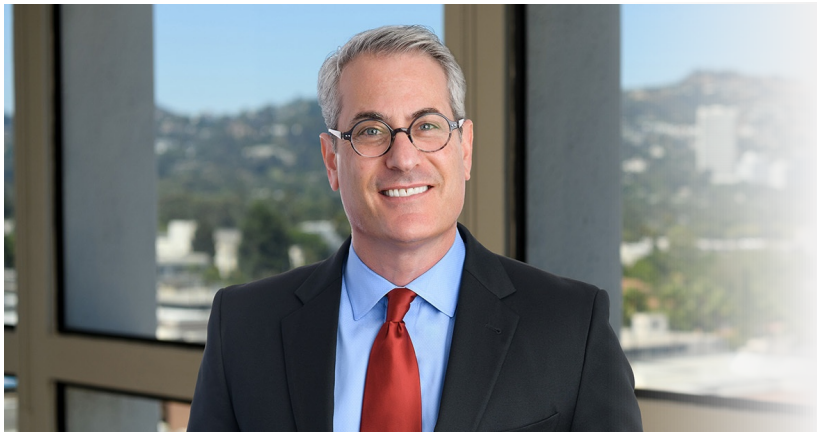
Do you do business in California and meet one or more of the following thresholds?

- Buy, sell, share, or receive for commercial purposes the personal information of 50,000 or more consumers, households, or devices
- Have an annual gross revenue in excess of $25 million
- Derive 50% or more of your annual revenue from selling consumer's personal information

YOU MUST COMPLY WITH THE CCPA

Contact Jeffrey R. Glassman at jglassman@ecjlaw.com with questions.

Ervin Cohen & Jessup LLP



Jeffrey R. Glassman

Partner

jglassman@ecjlaw.com
Direct 310.281.6302

Jeffrey has spent the last two decades working as a corporate attorney representing entrepreneurs, investors, start-ups, emerging growth and lower middle-market companies. During the dot com boom, Jeffrey was in-house counsel to a software development company in Silicon Valley. While in-house he negotiated complex technology licensing agreements, assisted the sales team with structuring deals, supervised the development and protection of the company's intellectual property ("IP") portfolio, implemented stock options plans and negotiated executive employment packages to recruit high-level talent, managed the company's efforts to comply with complex employment laws and regulations, and helped close a $35 million round of financing.

Jeffrey counsels clients on choice, formation, legal mechanics and organization of corporate entities, limited liability companies and partnerships; corporate governance and compliance, advising the Board of Directors, and shareholder and investor rights and liabilities; raising capital including angel and venture financing; compliance with federal and state securities laws and private placement memoranda; employment agreements; stock option and phantom equity plans and agreements; protection of IP and trade secrets, proprietary information; contracts and general business matters; and mergers and acquisitions, recapitalizations, and other exit strategies; the development and protection of IP portfolios; and a wide variety of business transactions and disputes.

He also advises clients on issues related to the Digital Millennium Copyright Act; domain names and trademarks; website, mobile app and software development; cloud, hosting, information technology and data security agreements and transactions; terms of use and legal issues related to social networking; the California Consumer Privacy Act of 2018, the EU's General Data Protection Regulation and related privacy laws and policies; e-commerce transactions; strategic alliance and joint venture agreements; advertising on the Internet; cybersecurity; and acquisition and sales of Internet-based businesses.

In addition, Jeffrey advises clients on a wide variety of transactional, regulatory and litigation matters including, but not limited to, issues related to cutting-edge Internet, mobile marketing, social media, viral and influencer marketing; keyword and other search issues; false advertising claims, how to ensure use of truthful communications with consumers; endorsements and testimonials in advertising, product promotion and placement, and disclosures of material connections with endorsers and influencers; native advertising and the subtle integration of brand and marketing messages into digital content; tracking of consumers' online and mobile activities; and compliance with FTC guidelines and the CAN-SPAM Act.

Education

J.D., American University, Washington College of Law, *Dean's Fellow*

B.A., University of Wisconsin, Madison, *With Distinction*

Practice Areas

Business, Corporate and Tax

Intellectual Property and Technology

Admissions

California

Maryland

District of Columbia

Affiliations

Los Angeles County Bar Association, Co-Chair of Programs, Executive Committee

Entertainment Law and Intellectual Property Section

ProVisors (Professional Association of Trusted Advisors)