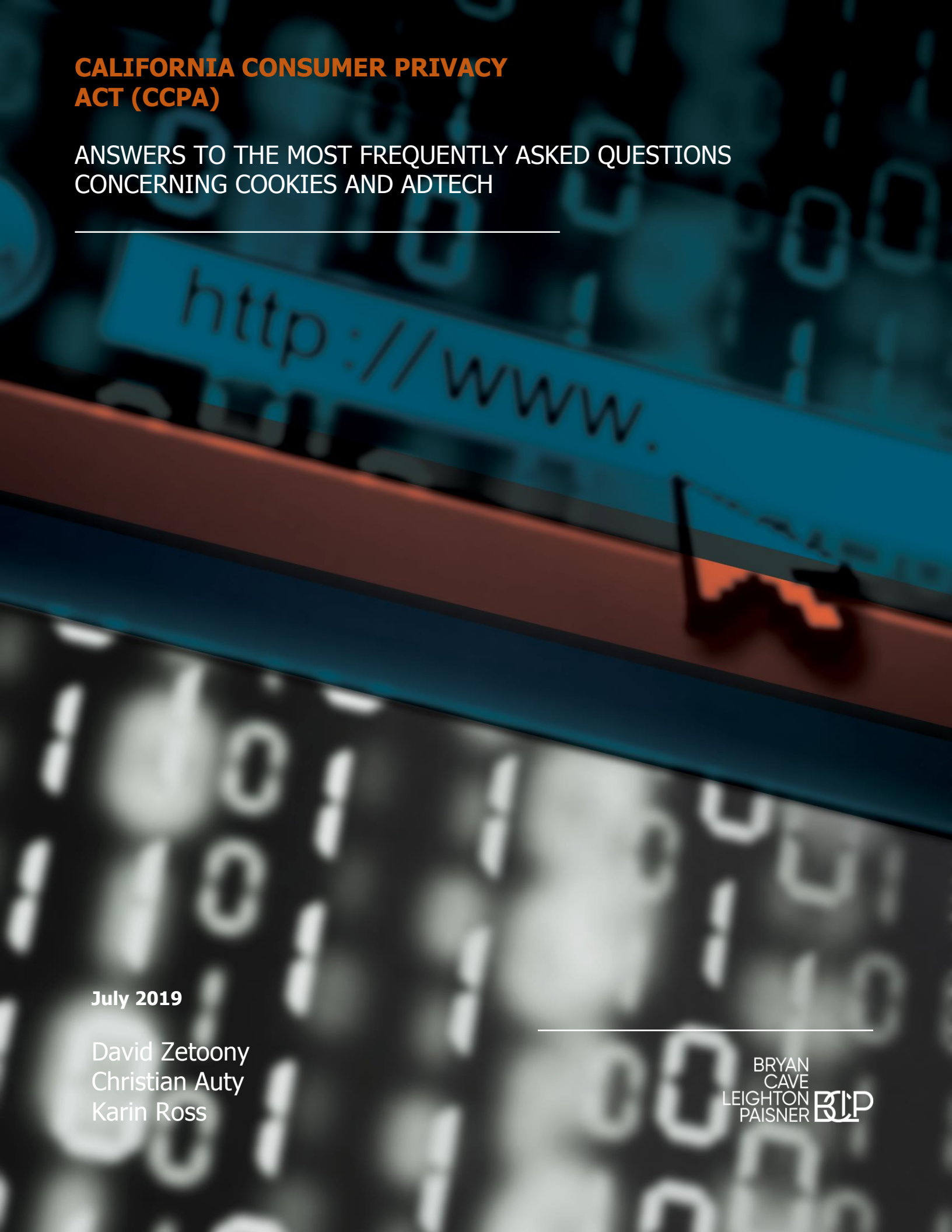


CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

ANSWERS TO THE MOST FREQUENTLY ASKED QUESTIONS CONCERNING COOKIES AND ADTECH

July 2019

David Zetoony
Christian Auty
Karin Ross

BRYAN CAVE LEIGHTON PAISNER BCLP

Content

Introduction 1

FAQ. 1 Is a cookie considered "personal information"? 2

FAQ. 2 What is the difference between a "first party cookie" and a "third party cookie"? 3

FAQ. 3 Does the CCPA require a cookie banner when a company uses first-party session cookies? 4

FAQ. 4 Does the CCPA require that a company obtain consent from a website user before placing cookies on their browser? 5

FAQ. 5 Does the CCPA require that a company allow consumers to opt-out (e.g., toggle off) essential cookies? 6

FAQ. 6 Does the CCPA require that a company allow consumers to opt-out (e.g., toggle off) analytics cookies? 7

FAQ. 7 If a company collects personal information through a cookie is it required to provide a consumer with a privacy policy? 10

FAQ. 8 If a website participates in behavioral advertising, does the CCPA require that it disclose that it is "selling" consumers' information? 12

FAQ. 9 If a website participates in behavioral advertising, does Nevada's privacy law require that THE WEBSITE disclose that it is "selling" consumers' information? 15

FAQ. 10 Will the CCPA lead websites to have EU-style cookie banners? 17

FAQ. 11 What are the different types of cookie banner? 18

FAQ. 12 What impact do different types of cookie banners have on CCPA compliance when utilizing third party behavioral advertising? 19

FAQ. 13 If I post a "do not sell my personal information" link on my website, and opt those consumers that select it from receiving behavioral advertising cookies, have I complied with the CCPA? 22

FAQ. 14 Is there a private right of action for failing to disclose the "sale" of information to third party behavioral advertisers? 23

FAQ. 15 What is the statutory penalty for a violation of the CCPA? 24

Text of the CCPA 25

Data privacy and security team 46



David Zetoony
Partner
Chair, Data Privacy and Security Team
T: +1 303 417 8530
david.zetoony@bclplaw.com

INTRODUCTION

When the CCPA was enacted last year BCLP published a Practical Guide to help companies reduce the requirements of the Act into practice. Following publication of the Guide we wrote a series of articles that addressed companies' most frequently asked questions concerning the CCPA. The Guide, and the FAQ series, contributed to JD Supra naming BCLP as the 2019 "Top" law firm in the area of Data Collection & Data Use (i.e., data privacy).

There is a great deal of confusion surrounding what impact the CCPA will have on the use of cookies – and in particular third party behavioral advertising cookies. In order to address that topic, we have collected our cookies-related FAQs and have republished them here as a "handbook" that companies can use when trying to understand the impact that the CCPA will have on their use of first and third party cookies, as well as behavioral advertising networks. The articles also help explain the impact that the CCPA will have on the AdTech world in general. We hope that you find this a valuable resource.

Sincerely,



David Zetoony

Bryan Cave Leighton Paisner

Chair Global Data Privacy and Security Practice



FAQ. 1 IS A COOKIE CONSIDERED "PERSONAL INFORMATION"?

The terms "personal data," "personal information," or "personally identifiable information" are used in various statutes and regulations in different contexts and are assigned different meanings. For example, the term "personal information" is defined under most state data breach notification statutes as referring only to name in combination with a small sub-set of data fields viewed by legislators as being particularly sensitive, such as Social Security Number.

For the purpose of California's CCPA the phrase "personal information" refers to any 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."[1] The CCPA includes a non-exhaustive list of data types that fall within that definition. That list includes "unique personal identifiers,"[2] a term which itself is defined as including "cookies" that are used to "recognize a . . . device that is linked to a consumer or family, over time and across different services."[3] As a result, while cookies are not considered "personal information" in the context of most data privacy and security statutes, cookies (or at least persistent cookies) are considered "personal information" for the purposes of the CCPA.

Personal data is similarly defined by the European GDPR as "any information relating to an identified or identifiable natural person."[4] The Article 29 Working Party has taken the position that when a cookie "[i]s not linked to identifiable data of a specific person" it can be considered "anonymous."[5] Conversely, if a company links a cookie to an identifiable person the cookie becomes part of the set of "personal data." For example, the Working Party has opined that if a "customer fills an order form on the web site where the advertiser has placed the banner ad" then "identifiable data could be linked or merged with existing data already placed on a cookie, and provide for an identifiable profile of the person concerned."[6]

---

1 CCPA, Section 1798.140(o)(1).
2 CCPA, Section 1798.140(o)(1)(A).
3 CCPA, Section 1798.140(x).
4 GDPR, Article 4(1).
5 Article 29 Working Party, WP 37: Privacy on the Internet – An Integrated EU Approach to On-line Data Protection, at 74, adopted on Nov. 21, 2000.
6 Article 29 Working Party, WP 37: Privacy on the Internet – An Integrated EU Approach to On-line Data Protection, at 74, adopted on Nov. 21, 2000.

FAQ. 2 WHAT IS THE DIFFERENCE BETWEEN A "FIRST PARTY COOKIE" AND A "THIRD PARTY COOKIE"?

Generally speaking, cookies simply are data files saved to a user's computer. As discussed in FAQ. 1, certain cookies may qualify as "personal information" under the CCPA, since the CCPA defines "unique personal identifiers,"[7] to include "cookies" that are used to "recognize a . . . device that is linked to a consumer or family, over time and across different services."[8]

Some cookies allow websites to perform essential functions, like remembering which products you selected for purchase and placed into your shopping cart. These cookies are often referred to as "essential" cookies. Other cookies feed information to retailers, site operators or others who have an interest in which sites a browser visited or other activity on the web browser. These are often referred to as "analytics" cookies. A third category of cookies are designed to facilitate targeted advertising to a consumer by tracking a web browser's viewing behaviour and/or correlating that viewing behaviour with other information known about the browser or the consumer that likely controls the browser. These are often referred to as "advertising" cookies or "behavioral advertising" cookies. In each case, cookies are simply data files stored on a computer.

What distinguishes a "first party" cookie from a "third party" cookie is the identity of the entity or website storing the cookie on the computer. In the case of "first party" cookies, this is the entity or site that is being visited. For example, a cookie that remembers the previous high score in a game may be installed only on the site on which the game is played.

"Third party" cookies, by contrast, are data files installed by another program (typically an advertisement that is presented on the site but is not owned or controlled by the site owner) or that is separate and distinct from the site that is being visited. Third party cookies are frequently used by advertising agencies and other entities to track users' activity across sites and over a longer period of time.

---

7 CCPA, Section 1798.140(o)(1)(A).

8 CCPA, Section 1798.140(x).

FAQ. 3 DOES THE CCPA REQUIRE A COOKIE BANNER WHEN A COMPANY USES FIRST-PARTY SESSION COOKIES?

No.

The CCPA defines "personal information" to include (among other things) a "unique identifier."[9] The phrase "unique identifier" is, in turn, defined as follows:

> "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.[10]

The first part of the above definition refers only to identifiers that can recognize a device "over time and across different services." This would not include session cookies designed to contain information only during a single online session (i.e., not over any significant length of time) and typically on a single website or domain (i.e., not across services). The second part of the definition, however, refers to cookies, and does so in a manner in which it is not clear whether cookies are included as a stand-alone category of "unique identifiers" or as an example of a type of identifier that may be able to recognize a device "over time and across different services." The first interpretation would mean that first-party session cookies are "personal information" governed by the CCPA; the second interpretation would mean that first-party session cookies are typically not "personal information" governed by the CCPA. The net result is that there is ambiguity as to whether the CCPA governs first-party session cookies at all.

Assuming that the CCPA is interpreted as applying to first-party session cookies, a company is required to disclose the use of such cookies in the company's online privacy policy.[11] The CCPA does not mandate that the use of cookies be disclosed in real time as part of a cookie banner, or that the company obtain consent prior to the use of cookies.

---

9 CCPA, Section 1798.140(o)(1).
10 CCPA, Section 1798.140(x).
11 CCPA, Section 1798.130(a)(5)(B).

FAQ. 4 DOES THE CCPA REQUIRE THAT A COMPANY OBTAIN CONSENT FROM A WEBSITE USER BEFORE PLACING COOKIES ON THEIR BROWSER?

No.

The CCPA does not expressly require that a company obtain consent from a website user before placing cookies on their browser. While consent is not expressly required, as discussed in FAQ. 8, in order to mitigate the risk that the use of third party behavioral advertising could be considered a "sale" many businesses may seek consent from users before deploying third party behavioral advertising cookies.

FAQ. 5 DOES THE CCPA REQUIRE THAT A COMPANY ALLOW CONSUMERS TO OPT-OUT (E.G., TOGGLE OFF) ESSENTIAL COOKIES?

No.

As is discussed in FAQ. 2, some cookies perform essential functions for the operation of a website, like remembering which products are selected for purchase and placed into a shopping cart. If those "essential" cookies are placed by a business directly (e.g., first-party essential cookies) the CCPA does not require that a business provide consumers the ability to turn them off. If those essential cookies are placed by a third party on behalf of a business, so long as the third party is considered a "service provider" under the CCPA (i.e., the contract with the third party has use, disclosure and retention prohibitions) the CCPA also does not require that a business provide consumers the ability to turn them off. The net result is that under the CCPA businesses typically do not have to give consumers control over essential cookies.

FAQ. 6 DOES THE CCPA REQUIRE THAT A COMPANY ALLOW CONSUMERS TO OPT-OUT (E.G., TOGGLE OFF) ANALYTICS COOKIES?

It depends.

The CCPA requires that a business that "sells" personal information disclose within its privacy policy a "list of the categories of personal information it has sold about consumers in the preceding 12 months."[12] The CCPA broadly defines the term "sell" as including the act of "disclosing" or "making available" personal information "for monetary or other valuable consideration."[13] "Personal information" is also defined broadly as including any information that "could reasonably be linked, directly or indirectly, with a particular consumer or household" such as, in certain instances, IP addresses, unique online identifiers, browsing history, search history and "information regarding a consumer's interaction with an Internet Web site, application, or advertisement."[14]

While the definition of "sale" under the CCPA contains an exception for situations in which information is shared with a service provider, whether the exception applies to analytics cookies operated by third parties may depend in part upon the contract in place (or terms and conditions) with the third party.[15] Specifically, the service provider exception requires that the following three conditions be present:

1. The transfer of information to the service provider must be "necessary" for the website's business purpose.[16] It is uncertain whether a court would view analytics cookies (and the information that they provide) as a necessity.

2. The transfer of the information to the service provider must be disclosed to consumers. Many websites arguably meet this requirement by disclosing their use of third party cookies or analytics cookies in their privacy policies.

3. The agreement with a service provider must "prohibit" the service provider "from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract with the business."[17] Whether the

---

12 CCPA, Section 1798.130(A)(5)(C)(i).
13 CCPA, Section 1798.140(t)(1).
14 CCPA, Section 1798.140(o)(1)(A), (F).
15 CCPA, Section 1798.140(t)(2)(C).
16 CCPA, Section 1798.t)(2)(C).
17 CCPA, Section 1798.140(t)(2)(C)(ii), (v).

contract in place with the provider of an analytics cookie meets these requirements may be a case-by-case inquiry.

In order to mitigate the risk that permitting analytics cookies to deploy on a website will be interpreted as a "sale" of information, a website has at least three options:

1. Verify that the contract fits the definition of a "service provider." If the analytics cookies is necessary for the efficient operation of the website, and if a website verifies that its contract with the analytics cookie provider qualifies as a "service provider," the cookie can be placed without offering consumers the ability to opt-out or toggle the cookie off.

2. Ask for consent. The CCPA excepts from the definition of "sale" the situation where a "consumer uses or directs the business to intentionally disclose personal information."[18] As a result, if a website deploys a cookie banner, and a consumer agrees or "opts-in" to the use of analytics cookies, the website arguably has not "sold" information to the company that provides the analytics cookie. Note that if the consumer agrees to the deployment of the analytics cookie, nothing within the CCPA would require the website to present them with an ability to later opt-out (i.e., toggle off) the cookie.

3. Disclose the sale of information and offer opt-out. If an analytics vendor does not fit the definition of a "service provider," and opt-in consent is not obtained, a website could disclose within its privacy policy that it is "selling" information (as that term is defined within the CCPA) to an analytics cookie provider. Note, however, that if a company sells personal information, the CCPA requires that the company provide a "Do Not Sell My Personal Information" link on its homepage, and honor requests to opt-out from such sales.[19] Assuming that a business provides such a link, it is not clear that a mechanism currently exists for the business to communicate to analytics cookie providers that a particular consumers' information cannot be collected. One possible alternative might be to adopt a cookie management tool that provides consumers with the ability to "toggle off" the analytics cookie. A cookie management tool solution, however, has not been validated by the California Attorney General or by California courts and may raise conceptual questions concerning whether the "toggle-off" feature is

---

18 CCPA, Section 1798.140(t)(2)(A).

19 CCPA, Section 1798.135(a)(1).

sufficient given that the consumer may be re-presented with a request to accept analytics cookie the next time that the consumer clears their cache, or visits the website from a different browser.

The net result is that while the CCPA does not expressly require that websites offer to consumers the ability to "toggle-off" analytics cookies, some companies may offer such a feature as part of a risk mitigation strategy.

FAQ. 7 IF A COMPANY COLLECTS PERSONAL INFORMATION THROUGH A COOKIE IS IT REQUIRED TO PROVIDE A CONSUMER WITH A PRIVACY POLICY?

Maybe.

Section 1798.100(b) of the CCPA states that a "business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used." Plaintiffs and consumer advocates are likely to argue that this requirement applies to information collected through "cookies" based upon the following:

- The CCPA defines the term "collects" as including situations in which a business "buy[s], rent[s], gather[s], obtain[s], receiv[es], or access[es]" personal information by "any means."[20]

- The CCPA defines "personal information" to include "unique identifiers" which includes "persistent identifier[s] that can be used to recognize a . . . device that is linked to a consumer . . . over time and across different services, including, but not limited to . . . cookies."[21]

It is worth noting, however, that notifying a consumer about the type of information collected and the purpose of the collection does not *necessarily* mean distributing to the consumer a full privacy policy. The statute does not require, for example, that the notification must be in writing or that the notification must include other types of information that are typically present in a privacy notice (e.g., information on the company's practices with regard to sharing, etc.). As a result, it is possible that a company that collects information across websites through the use of cookies is able to fulfill its obligation to inform consumers of the data that it collects and its use for that data orally, contextually, or via a third party (e.g., via the privacy policy of company A that might intend to transmit the information to company B).

Some companies that collect information across websites through the use of cookies (i.e., third party behavioral advertisers) may also take the position that their cookies do not fall within the definition of "unique identifier" (and, through that, the definition of "personal information") because their cookies are not "persistent." For example, they may argue that if their cookie is set to expire in 90 days or 60 days it should be considered transient in nature. California's courts and the California Office of the Attorney General have not interpreted whether cookies

---

20 CCPA, 1798.140(e)

21 CCPA, 1798.140(x)

with set expiration dates should be considered "persistent" for the purposes of the CCPA.

FAQ. 8 IF A WEBSITE PARTICIPATES IN BEHAVIORAL ADVERTISING, DOES THE CCPA REQUIRE THAT IT DISCLOSE THAT IT IS "SELLING" CONSUMERS' INFORMATION?

The California CCPA requires that a business that "sells" personal information disclose within its privacy policy a "list of the categories of personal information it has sold about consumers in the preceding 12 months."[22] The CCPA broadly defines the term "sell" as including the act of "disclosing" or "making available" personal information "for monetary or other valuable consideration."[23] "Personal information" is also defined broadly as including any information that "could reasonably be linked, directly or indirectly, with a particular consumer or household" such as, in certain instances, IP addresses, unique online identifiers, browsing history, search history and "information regarding a consumer's interaction with an Internet Web site, application, or advertisement."[24]

Many companies – particularly online retailers – participate in behavioral advertising networks. In order to participate in a network, a company places code on its website that permits a third party (the behavioral advertising network) to either (1) place tracking technology (e.g., a cookie) on the computer of people who visit the website, or (2) receive information that the visitor's computer transmits to the website that the visitor intends to visit. This might include, for example, a GET request whereby the consumer's computer asks the website to load a webpage, or a POST submission whereby the consumer transmits information about themselves (e.g., email address, search query, etc.) to the website. The third party behavioral advertising network collects and aggregates the information in order to monitor a consumer (or at least the consumer's computer) across all of the websites that participate in the network and to build a profile from which the behavioral advertising provider can discern characteristics about the consumer to help deliver targeted advertising.

Unrelated to the CCPA, courts that have evaluated the relationship between a consumer, the website that they intend to visit, and behavioral advertising networks that receive information about that visit have held that the data transmitted from the consumer to the website is "intended for" the website itself, and the website is, in turn, "consent[ing]" for the behavioral advertising network to "access" consumers' "communications to them."[25] In other words, they view the website as "authoriz[ing]" a behavioral advertising network to access information

---

22 CCPA, Section 1798.130(A)(5)(C)(i).
23 CCPA, Section 1798.140(t)(1).
24 CCPA, Section 1798.140(o)(1)(A), (F).
25 *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 511 (S.D.N.Y. 2001).

transmitted by a consumer to the website.[26] Given the precedent, plaintiffs' attorneys are likely to argue that the act of authorizing a third party behavioral network to access information transmitted by a consumer is synonymous with "making available" the information and, thus, constitutes a "sale" pursuant to the CCPA.

While the definition of "sale" under the CCPA contains an exception for situations in which information is shared with a service provider, the exception may not apply to behavioral advertising networks.[27] Specifically, the service provider exception requires that three conditions be present. While some of those conditions exist in the context of a behavioral advertiser, others do not.

First, the transfer of information to the service provider must be "necessary" for the website's business purpose.[28] While the facilitation of targeted advertising may be desirable, it is questionable whether a court would view targeted advertising as a necessity.

Second, the transfer of the information to the service provider must be disclosed to consumers. Many websites arguably meet this requirement by disclosing their participation in behavioral advertising networks within their privacy policies.

Third, the agreement with a service provider must "prohibit" the service provider "from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract with the business."[29] As behavioral advertising networks typically retain the information that they obtain from websites within their network, and use that information for the benefit of themselves (and the other members of their network) a plaintiff's attorney is likely to argue that the contracts in-place between websites and advertising networks are insufficient to convert the advertising network into a "service provider."

In order to mitigate the risk that permitting behavioral advertising networks to deploy cookies on a website will be interpreted as a "sale" of information, a website has two main options:

- Ask for consent. The CCPA excepts from the definition of "sale" the situation where a "consumer uses or directs the business to intentionally disclose personal information."[30] As a result, if a website deploys a cookie

---

26 *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001).
27 CCPA, Section 1798.140(t)(2)(C).
28 CCPA, Section 1798.t)(2)(C).
29 CCPA, Section 1798.140(t)(2)(C)(ii), (v).
30 CCPA, Section 1798.140(t)(2)(A).

banner, and a consumer agrees or "opts-in" to the use of tracking cookies, the website arguably has not "sold" information to behavioral advertisers.

- Disclose the sale of information and offer opt-out. If opt-in consent is not obtained, a website could disclose within its privacy policy that it is "selling" information (as that term is defined within the CCPA) to behavioral advertising networks. Note, however, that if a company sells personal information, the CCPA requires that the company provide a "Do Not Sell My Personal Information" link on its homepage, and honor requests to opt-out from such sales.[31] Assuming that a business provides such a link, it is not clear that a mechanism currently exists for the business to communicate to the behavioral advertising networks that a particular consumers' information cannot be collected, or to ensure that consent to transfer the information is not re-solicited each time the consumer clears their cache or visits the website from a different computer or browser.

[31] CCPA, Section 1798.135(a)(1).

FAQ. 9 IF A WEBSITE PARTICIPATES IN BEHAVIORAL ADVERTISING, DOES NEVADA'S PRIVACY LAW REQUIRE THAT THE WEBSITE DISCLOSE THAT IT IS "SELLING" CONSUMERS' INFORMATION?

On May 29, 2019, Nevada became the first state to pass legislation emulating portions of the CCPA when it adopted Senate Bill No. 220.

While Senate Bill No. 220 incorporates the CCPA's concept of permitting consumers to object to the sale by a company of their information, it avoids many of the drafting errors, ambiguities, and business impracticalities of the CCPA including its treatment of online behavioral advertising.

For context, and as is discussed in FAQ. 8, the California CCPA requires that a business that "sells" personal information disclose within its privacy policy a "list of the categories of personal information it has sold about consumers in the preceding 12 months."[32] The CCPA broadly defines the term "sell" as including the act of "disclosing" or "making available" personal information "for monetary or other valuable consideration."[33] "Personal information" is also defined broadly as including any information that "could reasonably be linked, directly or indirectly, with a particular consumer or household" such as, in certain instances, IP addresses, unique online identifiers, browsing history, search history and "information regarding a consumer's interaction with an Internet Web site, application, or advertisement."[34] Plaintiffs' attorneys are likely to argue that the act of authorizing a third party behavioral network to access information transmitted by a consumer is synonymous with "making available" the information and, thus, constitutes a "sale" pursuant to the CCPA. In order to mitigate the risk that permitting behavioral advertising networks to deploy cookies on a website will be interpreted as a "sale," many websites are asking consumers for opt-in consent to the use of behavioral advertising cookies through cookie banners. The CCPA excepts from the definition of "sale" the situation where a "consumer uses or directs the business to intentionally disclose personal information."[35] As a result, if a website deploys a cookie banner, and a consumer agrees or "opts-in" to the use of tracking cookies, the website arguably has not "sold" information to behavioral advertisers.

Unlike the CCPA, Nevada defines the term "sale" as including only "the exchange of covered information for monetary consideration by the operator [of a website] to a person for the person to license or sell the covered information to additional

---

32 CCPA, Section 1798.130(A)(5)(C)(i).
33 CCPA, Section 1798.140(t)(1).
34 CCPA, Section 1798.140(o)(1)(A), (F).
35 CCPA, Section 1798.140(t)(2)(A).

persons."[36] Nevada's narrower definition precludes the term from applying to the use of third party behavioral advertising networks as (1) behavioral advertising networks typically do not provide advertisers or publishers with "monetary consideration" for the deployment of their cookies, and (2) while the behavioral advertising networks may use the information that they obtain from their cookies for the benefit of themselves and their other clients, they typically do not "license or sell" that information.

---

[36] S.B. 220 at § 1.6.

FAQ. 10 WILL THE CCPA LEAD WEBSITES TO HAVE EU-STYLE COOKIE BANNERS?

Possibly.

The CCPA defines the phrase "personal information" to include any 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."[37] The CCPA includes a non-exhaustive list of data types that fall within that definition including "unique personal identifiers,"[38] a term that is itself defined to include "cookies" that are used to "recognize a . . . device that is linked to a consumer or family, over time and across different services."[39] As a result, the CCPA appears to treat persistent tracking cookies – such as those used by behavioral advertising networks – as "personal information" or a method of capturing "personal information." If a business collects "personal information" it is required under the CCPA to provide California residents with a privacy disclosure "at or before the point of [information] collection."[40]

In situations in which a website operator deploys its own persistent tracking cookie, the website can presumably provide a description of its privacy practices via its own privacy policy linked at the bottom of the website.

In situations in which a website deploys the tracking cookies of a third party (e.g., behavioral advertising network cookies), it is unclear how the business that owns and controls the tracking cookie (i.e., the behavioral advertising network) will be able to provide California consumers with its privacy disclosure "at or before the point" of information collection, unless the cookie-owner requires that any website that deploys its cookie provide a copy of the cookie-owner's privacy notice. This might be accomplished, for example, by requiring websites to deploy a cookie banner that contains links to the privacy notice of each cookie that deploys on the website.

---

37 CCPA, Section 1798.140(o)(1).
38 CCPA, Section 1798.140(o)(1)(A).
39 CCPA, Section 1798.140(x).
40 CCPA, Section 1798.100(b).

FAQ. 11 WHAT ARE THE DIFFERENT TYPES OF COOKIE BANNER?

The term "cookie banner" refers to a banner, or splash page, deployed on a website to inform visitors that the website uses cookies. There is little standardization concerning how cookie banners are deployed. Different websites position them in different places on the screen (e.g., top bar, bottom bar, or centered splash page), utilize different language to describe what cookies are, and use different terms to describe the options available to visitors. Generally, however, most cookie banners fall within three categories:

1. Notice Only. A "notice only" cookie banner discloses to visitors that the website deploys cookies, but does not give the website visitor any direct control concerning the use of cookies. In other words, the website visitor is not asked to permit / accept cookies, nor are they given a tool or mechanism for disabling cookies. Some notice-only cookie banners may, however, provide information to the visitor on how cookies can be disabled within the visitor's website browser.

2. Notice + Opt Out Consent. A "notice + opt out" cookie banner discloses to visitors that the website deploys cookies and provides the visitor with a mechanism for disabling the use of cookies on the website in the future. This may include a single option to "opt-out" of all cookies, or might provide a more granular option to opt-out of some types of cookies (e.g., behavioral advertising cookies) but no option with regard to other cookies (e.g., cookies necessary for the website to function).

3. Notice + Opt In Consent. A "notice + opt in consent" cookie banner discloses to consumers that the website would like to deploy cookies and asks the visitor to opt-in to the use of cookies *before* the cookies are deployed. This may include a single option to "opt in" to all cookies wherein no cookies will be placed on the browser absent consent, or it might provide a more granular option to opt-in to some types of cookies (e.g., behavioral advertising cookies), but no option with regard to other cookies (e.g., cookies necessary for the website to function).

FAQ. 12 WHAT IMPACT DO DIFFERENT TYPES OF COOKIE BANNERS HAVE ON CCPA COMPLIANCE WHEN UTILIZING THIRD PARTY BEHAVIORAL ADVERTISING?

As discussed in FAQ. 11, most cookie banners can be classified into one of three general categories: (1) notice only banners, (2) notice + opt-out banners, and (3) notice + opt-in banners. The type of cookie banner that a business uses may have a direct impact on what additional steps a business needs to take in order to achieve CCPA compliance. The following describes the practical effect that each type of cookie banner has in relation to CCPA obligations:

Type of Cookie Notice and Consent	Do you need to disclose that you have "sold" information to behavioral advertisers under the CCPA?	If you receive a deletion request do you need to forward it to the behavioral advertising company under the CCPA?	Do you need to include an "Opt Out of Sale" link pursuant to the CCPA?
Notice Only	Potentially. To the extent that a behavioral advertiser does not fall within the CCPA's definition of a "service provider," an argument might be made that the placement of the behavioral advertiser's cookie on a business's website constitutes a "sale" of information for which disclosure would be required.	No. Section 1798.105(c) only requires that a company forward a request to its "service providers." To the extent that the placement of the behavioral advertising cookie is considered a "sale" of information there would be no obligation to forward to the behavioral advertiser a deletion request.	Arguably yes. To the extent that the placement of the cookie is considered a "sale" section 1798.135 requires the posting of a "Do Not Sell My Personal Information" link.[41]
Notice + Opt-out consent	Potentially. To the extent that a behavioral advertiser does not fall within the CCPA's definition of a "service provider," an argument might be made that the placement of the behavioral	No. Section 1798.105(c) only requires that a company forward a request to its "service providers." To the extent that the placement of the behavioral advertising	Arguably yes. To the extent that the placement of the cookie is considered a "sale" section 1798.135 requires the posting of a "Do Not Sell My Personal Information" link.[43] While the consumer

[41] Note that posting a "do not sell my personal information link" on a website in a manner that allows consumers to prevent information from being shared with behavioral advertisers may not be possible in the context of current technology limitations and the requirements of the CCPA.

[43] Note that posting a "do not sell my personal information link" on a website in a manner that allows consumers to prevent information from being shared with behavioral advertisers

Type of Cookie Notice and Consent	Do you need to disclose that you have "sold" information to behavioral advertisers under the CCPA?	If you receive a deletion request do you need to forward it to the behavioral advertising company under the CCPA?	Do you need to include an "Opt Out of Sale" link pursuant to the CCPA?
	advertiser's cookie on a business's website constitutes a "sale" of information for which disclosure would be required. While there is an exception within the CCPA if a consumer "directs [a] business to intentionally disclose personal information" the CCPA states that "closing a given piece of content does not constitute a consumer's intent to interact with a third party."[42] In addition, the transfer would have occurred on page-load before a consumer would have had the ability to opt-out. While the consumer might have the ability to opt-out of future transfers after the page load, if the original transfer is considered a "sale," the sale cannot be undone.	cookie is considered a "sale" of information there would be no obligation to forward to the behavioral advertiser a deletion request.	may be able to avoid the future deployment of cookies by opting out on the cookie banner, the CCPA requires the "Do Not Sell My Personal Information" link to appear on the "Internet homepage" and to appear in the business's "online privacy policy."[44] The CCPA also requires a business to honor the opt-out request "for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information."[45]
Notice + Opt-in consent	Arguably no. Although there would be a transfer of information to a third party that has no limitation on how it will use the data, the CCPA includes an exception under its definition of "sale" for situations in which the "consumer uses or directs the business to intentionally	No. Section 1798.105(c) only requires that a company forward a request to its "service providers." To the extent that the placement of the behavioral advertising cookie was at the direction of the consumer, there would	Arguably no. The requirement to post a "Do Not Sell My Personal Information" link generally is not triggered where a consumer "directs the business to intentionally disclose personal information."[46]

may not be possible in the context of current technology limitations and the requirements of the CCPA.

42 CCPA, Section 1798.140(t)(2)(A).

44 CCPA, Section 1798.135(a)(1), (2)(A).

45 CCPA, Section 1798.135(a)(5).

46 CCPA, Section 1798.140(t)(2)(A).

Type of Cookie Notice and Consent	Do you need to disclose that you have "sold" information to behavioral advertisers under the CCPA?	If you receive a deletion request do you need to forward it to the behavioral advertising company under the CCPA?	Do you need to include an "Opt Out of Sale" link pursuant to the CCPA?
	disclose personal information." Note that while the consumer would have given their affirmative direction to disclose the information by opting-in, there remains some ambiguity as to whether the exception would apply as it requires that the third party recipient "does not also sell the personal information, unless that disclosure would be consistent with the provisions of [the CCPA]." 1798.140(t)(2)(A).	be no obligation to forward to the behavioral advertiser a deletion request.	

FAQ. 13 IF I POST A "DO NOT SELL MY PERSONAL INFORMATION" LINK ON MY WEBSITE, AND OPT THOSE CONSUMERS THAT SELECT IT FROM RECEIVING BEHAVIORAL ADVERTISING COOKIES, HAVE I COMPLIED WITH THE CCPA?

Arguably no.

As is discussed in FAQ. 8, while the definition of "sale" under the CCPA contains an exception for situations in which information is shared with a service provider, that exception may not apply to the extent that a behavioral advertising network is not contractually prohibited from using the personal information that it collects on a business's website for the benefit of itself or for the benefit of third parties (i.e., its other clients).[47] If courts determine that making personal information available to behavioral advertisers is a "sale," the CCPA would require the posting of a "Do Not Sell My Personal Information" link.[48]

Some businesses are considering providing a "do not sell my personal information" link on their homepage, which, when clicked, would activate a cookie management tool from which a consumer could indicate that they do not want third party behavioral advertising cookies to deploy on their browser. The use of a cookie management tool to opt a consumer out of behavioral advertising may not comply with all of the technical requirements of the CCPA, however. Specifically the CCPA requires that a business honor an opt-out request "for at least 12 months before requesting that the *consumer* authorize the sale of the consumer's personal information."[49] While a cookie management selection may persist for 12 months (or more) on the *browser* that the consumer used to initially access a website, a consumer could be resolicited to accept cookies before 12 months expire in the following situations:

- The consumer visits the website using a different browser (e.g., first visit in Chrome, second visit in Safari)
- The consumer visits the website from a different machine or device (e.g., first visit from laptop, second visit from smartphone), or
- The consumer clears their browser's cache.

---

47 CCPA, Section 1798.140(t)(2)(C).

48 Note that posting a "do not sell my personal information link" on a website in a manner that allows consumers to prevent information from being shared with behavioral advertisers may not be possible in the context of current technology limitations and the requirements of the CCPA.

49 CCPA, Section 1798.135(a)(5) (emphasis added).

FAQ. 14 IS THERE A PRIVATE RIGHT OF ACTION FOR FAILING TO DISCLOSE THE "SALE" OF INFORMATION TO THIRD PARTY BEHAVIORAL ADVERTISERS?

No.

Currently the CCPA only provides a private right of action to a consumer whose unencrypted sensitive-category information has been breached as a result of a business's violation of its duty to "implement and maintain reasonable security procedures and practices."[50] The Act does not provide for a private right of action for an alleged failure to disclose the sale of information, or an alleged failure to offer (or honor) an opt-out of the sale of information, and further states that "[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law."[51]

It is worth noting that amendments have been proposed to the CCPA which might allow a private right of action for *any* alleged violation of the statute. One of those amendments – Senate Bill 561 – is currently on hold within the Senate Appropriations Committee for an evaluation of its potential fiscal impact. It is possible that the Senate Bill may be enacted in 2020 after its fiscal impact has been evaluated.

---

50 CCPA, Section 1798.150(a)(1) (referring to those categories of personal information specified under Cal. Civil Code 1798.81.5(d)(1)(A).

51 CCPA, Section 1798.150(c).

FAQ. 15 WHAT IS THE STATUTORY PENALTY FOR A VIOLATION OF THE CCPA?

$2,500 for each violation and $7,500 for each intentional violation.

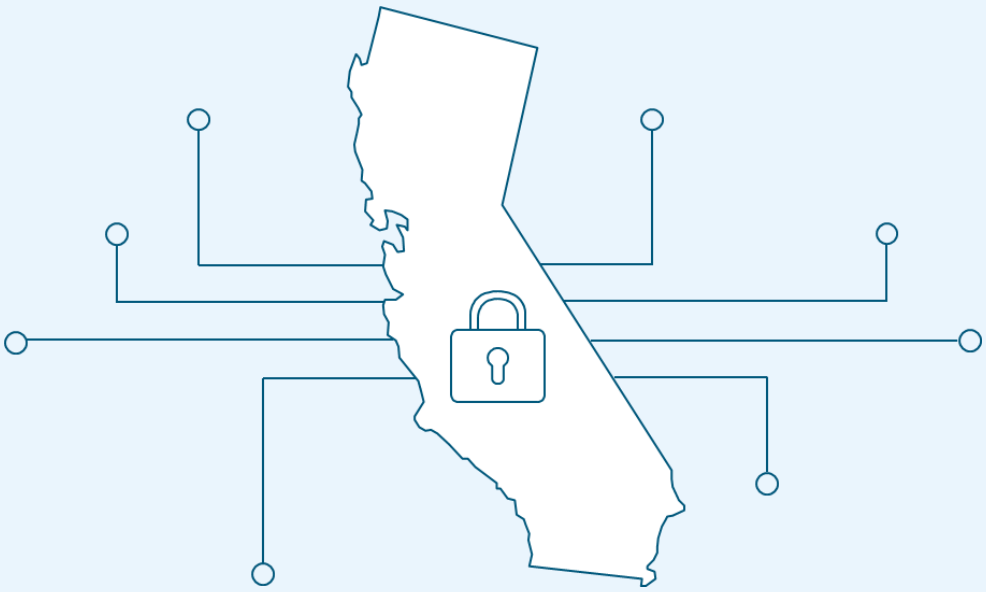
As discussed in FAQ. 14, the CCPA only provides a private right of action to any consumer whose unencrypted sensitive-category information has been breached as a result of a business's violation of its duty to "implement and maintain reasonable security procedures and practices." [52] But the California Attorney General may bring a civil action against any entity violating the act. Specifically, the CCPA provides that "[a]ny business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General."[53] The same section provides that these civil penalties may be assessed and recovered exclusively by the California Attorney General.

---

52 CCPA, Section 1798.150(a)(1) (referring to those categories of personal information specified under Cal. Civil Code 1798.81.5(d)(1)(A).

53 CCPA, Section 1798.155(b).

TEXT OF THE CCPA



Text of the California Consumer Privacy Act of 2018

(Last updated Sept. 23, 2018)

Table of Contents[54]

1798.100 - Consumers right to receive information on privacy practices and access information

1798.105 - Consumers right to deletion

1798.110 – Information required to be provided as part of an access request

1798.115 – Consumers right to receive information about onward disclosures

1798.120 – Consumer right to prohibit the sale of their information

1798.125 – Price discrimination based upon the exercise of the opt-out right

1798.130 – Means for exercising consumer rights

1798.135 – Opt-out link

1798.140 – Definitions

1798.145 – Interaction with other statutes, rights, and obligations

1798.150 – Civil actions

1798.155 - Attorney General guidance and enforcement

1798.160 - Consumer privacy fund

1798.175 - Intent, scope, and construction of title

1798.180 - Pre-emption

1798.185 - Adoption of regulations

1798.190 - Intermediate steps or transactions to be disregarded

1798.192 - Void and unenforceable provisions of contract or agreement

1798.194 - Liberal construction of title

1798.196 - Construction with federal law and California constitution

1798.198 - Operative date

---

[54] Section headings do not appear in the official version of the statute and were added by BCLP for ease and clarity.

1798.100 – Right to receive information on privacy practices and access information

(a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

1798.105 - Right to deletion

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

1798.110 – Substance of required disclosures

(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable request from the consumer.

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information the business has collected about that consumer.

(d) This section does not require a business to do the following:

(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

1798.115 - Right to receive access to information and information about onward disclosures

(a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose.

(b) A business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out pursuant to Section 1798.120.

1798.120 - Right to prohibit the sale of their information

(a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the right to opt out of the sale of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt in."

(d) A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal

information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

1798.125 - Price discrimination based upon the exercise of rights

(a)

(1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

(b)

(1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data.

(2) A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

1798.130 - Means for exercising consumer rights, and additional disclosure requirements

(a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall in a form that is reasonably accessible to consumers:

(1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the

required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.

(3) For purposes of subdivision (b) of Section 1798.110:

(A) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its Internet Web site, and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Sections 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

1798.135 – Opt out link

(a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(c) A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General.

1798.140 - Definitions

For purposes of this title:

(a) "Aggregate consumer information" means 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. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(b) "Biometric information" means an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.

(d) "Business purpose" means the use of personal information for the business' or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

(5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

(6) Undertaking internal research for technological development and demonstration.

(7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(e) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behaviour.

(f) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purposes" do not include for the purpose of

engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(h) "Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(2) Has implemented business processes that specifically prohibit reidentification of the information.

(3) Has implemented business processes to prevent inadvertent release of deidentified information.

(4) Makes no attempt to reidentify the information.

(i) "Designated methods for submitting requests" means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(j) "Device" means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

(k) "Health insurance information" means a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(l) "Homepage" means the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.145, including, but not limited to, before downloading the application.

(m) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(n) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(o)

(1) "Personal information" means 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. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behaviour, attitudes, intelligence, abilities, and aptitudes.

(2) "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used 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. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.

(p) "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(q) "Processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(r) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(s) "Research" means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health.

Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(4) Subject to business processes that specifically prohibit reidentification of the information.

(5) Made subject to business processes to prevent inadvertent release of deidentified information.

(6) Protected from any reidentification attempts.

(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(8) Not be used for any commercial purpose.

(9) Subjected by the business conducting the research to additional security controls limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

(t)

(1) "Sell," "selling," "sale," or "sold," means 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 by the business to another business or a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

(i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.

(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(u) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(v) "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, 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, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

(w) "Third party" means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2)

(A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

(i) Prohibits the person receiving the personal information from:

(I) Selling the personal information.

(II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract

(III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(B) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(3) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

(x) "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

(y) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

1798.145 - Interaction with other statutes, rights, and obligations

(a) The obligations imposed on businesses by this title shall not restrict a business's ability to:

(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 aggregate consumer information.

(6) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c)

(1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5)

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) This title shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined by subdivision (d) of Section 1681a of Title 15 of the United States Code, and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) Notwithstanding a business's obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

(h) A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.

(i) This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(j) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.

(k) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

1798.150- Civil actions

(a)

(1) Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case,

including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

1798.155 - Attorney General guidance and enforcement

(a) Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.

(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(c) Any civil penalty assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (b), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

1798.160 - Consumer privacy fund

(a) A special fund to be known as the "Consumer Privacy Fund" is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature to offset any costs incurred by the state courts in connection with actions brought to enforce this title and any costs incurred by the Attorney General in carrying out the Attorney General's duties under this title.

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively to offset any costs incurred by the state courts and the Attorney General in connection with this title. These funds shall not be subject to appropriation or transfer by the Legislature for any other purpose, unless the Director of Finance determines that the funds are in excess of the funding needed to fully offset the costs incurred by the state courts and the Attorney General in connection with this title, in which case the Legislature may appropriate excess funds for other purposes.

1798.175 - Intent, scope, and construction of title

This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

1798.180 -Preemption

This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

1798.185 - Adoption of regulations

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt out of the sale of personal information pursuant to paragraph (1) of subdivision (a) of Section 1798.145.

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary threshold in subparagraph (A) of paragraph (1) of subdivision (c) of Section 1798.140 in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business' determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(b) The Attorney General may adopt additional regulations as necessary to further the purposes of this title.

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

1798.190 - Intermediate steps or transactions to be disregarded

If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.

1798.192 - Void and unenforceable provisions of contract or agreement

Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt out of a business' sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

1798.194 - Liberal construction of title

This title shall be liberally construed to effectuate its purposes.

1798.196 - Construction with federal law and California constitution

This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

1798.198 - Operative date

(a) Subject to limitation provided in subdivision (b), and in Section 1798.199, this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

1798.199 - Operative date

Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

DATA PRIVACY AND SECURITY TEAM



David Zetoony
Partner / Chair Privacy Team
Boulder, Colorado
T: +1 303 417 8530
david.zetoony@bclplaw.com



Kate Brimsted
Partner
London, England
T: +44 (0)20 3400 3207
kate.brimsted@bclplaw.com



Sarah Delon-Bouquet
Counsel
Paris, France
T: +33 (0) 1 44 17 77 25
sarah.delonbouquet@bclplaw.



Jena Valdetero
Partner
Chicago, Illinois
T: +1 312 602 5056
jena.valdetero@bclplaw.com



Dominik Weiss
Counsel
Hamburg, Germany
T: +49 (0) 40 30 33 16 148
dominik.weiss@bclplaw.com



Nicola Conway
Associate
London, England
T: +44 (0) 20 3207 1312
nicola.conway@bclplaw.com



Tom Evans
Associate
London England
T: +44 (0)20 3400 2661
tom.evans@bclplaw.com



Jason Haislmaier
Partner
Boulder, Colorado
T: +1 303 417 8503
jason.haislmaier@bclplaw.com



Josh James
Associate
Washington D.C.
T: +1 202 508 6265
josh.james@bclplaw.com



Andrew Klungness
Partner
Santa Monica, California
T: +1 310 576 2176
andrew.k@bclplaw.com



Carolyn Krampitz
Associate
Hamburg, Germany
T: +49 (0) 40 30 33 16 149
carolyn.krampitz@bclplaw.co



Emmanuelle Mercier
Associate
Paris France
T: +33 (0) 1 44 17 77 74
emmanuelle.mercier@bclplaw.



François Alambret
Counsel
Paris, France
T: +33 (0) 1 44 17 77 48
francois.alambret@bclplaw.co



Jessica Pedersen
Associate
Chicago, Illinois
T: +1 312 602 5027
jessica.pedersen@bclplaw.com



Karin Ross
Associate
Boulder, Colorado
T: +1 303 417 8511
karin.ross@bclplaw.com



Tyler Thompson
Associate
Boulder Colorado
T: +1 303 866 0231
tyler.thompson@bclplaw.com



Maria Vathis
Of Counsel
Chicago, Illinois
T: +1 312 602 5127
maria.vathis@bclplaw.com



Serena Yee
Counsel
St. Louis, Missouri
T: +1 314 259 2372
sfyee@bclplaw.com



Kevin Scott
Counsel
Chicago, Illinois
T: +1 312 602 5074
kevin.scott@bclplaw.com

Christian Auty
Counsel
Chicago, Illinois
T: +1 312-602-5144
Christian.Auty@bclplaw.com

Getting in touch

When you need a practical legal solution for your next business opportunity or challenge, please get in touch.

David Zetoony
Tel: +1 303 417 8530
david.zetoony@bclplaw.com