CALIFORNIA CONSUMER PRIVACY ACT

THE LITIGATOR’S HANDBOOK: ANSWERS TO THE TOP 50 FREQUENTLY ASKED QUESTIONS CONCERNING LITIGATION AND THE CCPA

February 2020

David Zetoony, Partner
Jena Valdetero, Partner
Jennifer Jackson, Partner
Anne Redcross Beehler, Associate
Goli Mahdavi, Associate

BRYAN CAVE LEIGHTON PAISNER

Content

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

Jena Valdetero
Partner
Chair, Data Security Team
T: +1 312-602-5056
Jena.Valdetero@bryancave.com

INTRODUCTION

When the CCPA was enacted 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), and Lexology naming BCLP as the top "Though Leader" for technology, media, and telecommunications law (which includes data privacy and security).

The biggest CCPA risk, bar none, are data security breach related class action lawsuits.

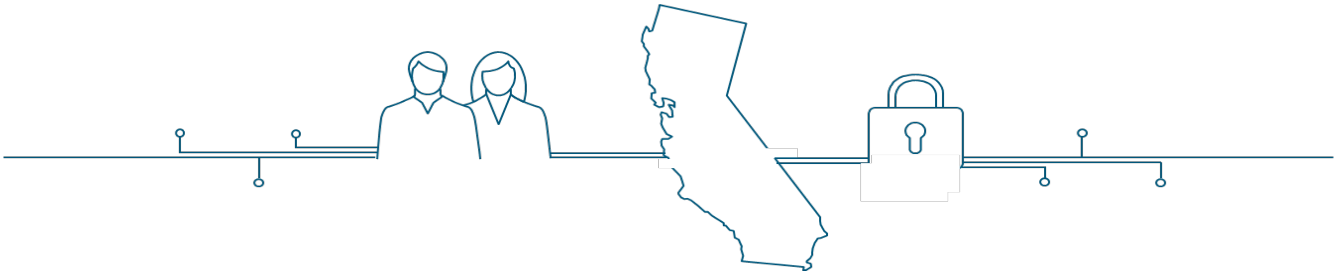
BCLP has a unique vantage point when it comes to class actions. We have one of the largest and most respected class action defence practices in the country. 225 of our attorneys handled over 400 class actions in just the past five years. We use that knowledge base to provide not only our clients with the best information on how to avoid, and defend, data security class actions, but to help educate the larger defense bar as well. Indeed in the last year alone 2,158 law firms – from the AmLaw 100 to solo practitioners – downloaded BCLP's data privacy and security resources as they endeavoured to advise or represent their own clients on complex data security issues. Lawyers at other firms have also cited BCLP's data security opinions when briefing data security topics to circuit courts and to the United States Supreme Court.

We hope that this handbook continues to provide our clients and the industry with the information needed to understand and defend data security class actions.

Sincerely,

Jena Valdetero & David Zetoony

Chairs Global Data Privacy & Security Practices



FAQ. 1 WHAT IS A "CONSUMER" AS SET FORTH IN THE CCPA?

The data privacy and security laws in the United States use different words to describe the individuals about whose information the laws apply. These include terms such as "covered person,"[1] "individual,"[2] and "customer."[3] The term used in a particular statute is less important than is its definition. For example, two statutes may use the term "individual," but one may define it as referring to all natural persons whereas another may define it as only referring to natural persons that are resident within the state. As another example, one statute may use the term "covered person" while another uses the term "individual," and yet they define the terms in an identical manner.

The CCPA uses the term "consumer" to refer to the individuals whose information is governed by the statute. While the common definition of "consumer" suggests that it refers to an individual that has "consumed" a product or a service in relation to a company, the definition ascribed by the CCPA is far broader. The term is defined to include any "natural person who is a California resident."[4] Read literally, the phrase might include not only an individual that consumes a product (e.g., a customer of a store), but also that store's California-based employees and California-based business contacts or prospective customers.

From a litigation standpoint, the broad definition of "consumer" means that plaintiffs' attorneys are gearing up to use the CCPA to bring cases on behalf of myriad different groups about whom companies typically hold information including, for example:

- End-use customers,
- Employees,
- Shareholders, and
- Service providers and vendors.

[1] *See*, e.g., Alaska Data Breach Notification Statute, Alaska Code Section 45.48.090(2).

[2] *See, e.g.,* Arizona Data Breach Notification Statute, Arizona Code Section 44-7501(L)(4).

[3] *See, e.g.,* Arkansas Data Breach Notification Statute, Arkansas Code Section 44-110-103(3);
California Data Breach Notification Statute, Cal. Civil Code 1798.80(c).

[4] CCPA, Section 1798.140(g).

FAQ. 2 WHAT DOES IT MEAN TO "DO BUSINESS" IN CALIFORNIA?

The CCPA purports to apply to any for-profit legal entity that "does business in the State of California" and that satisfies one of three thresholds:

1. Has annual gross revenue in excess of $25 million,
2. Purchases, receives for commercial purposes, sells, or shares for commercial purposes, personal information of 50,000 or more consumers, or
3. Derives 50% of its annual revenue from selling consumer personal information.[5]

For companies doing substantial business in California, determining whether they must comply is a relatively simple matter, as the Act establishes specific thresholds of economic and operational activity. However, for companies that have neither a physical presence in California nor significant numbers of employees that reside in California, making an assessment of whether one is "doing business" within the State can be more difficult. California personal jurisdiction jurisprudence provides some insights.

California's long-arm statute[6] permits the broadest possible exercise of jurisdiction, limited only by Constitutional considerations. Courts apply a liberal view as to the amount and kind of activities which will meet this standard. Unfortunately, there is no all-embracing rule governing what constitutes "doing business" in the State, and the question is one of fact. Until the Attorney General's office provides guidance, the following factors provide some indication of how a court could determine the issue:

- Intentional - not merely fortuitous - economic activity within the State is likely sufficient to constitute "doing business."
- One or two isolated transactions is typically not enough to constitute "doing business."
- Entering into a contract with a California entity does not necessarily constitute "doing business" in California.
- An entity's lack of physical presence in the State is not determinative of whether the entity is "doing business" in the State.
- Maintenance of a passive website alone is likely not enough, but in conjunction with something more, like site content specifically targeting California residents, a company could be found to be "doing business" in California.

[5] CPPA, Section 1798.140(c)(1)(A)-(C).

[6] Code Civ. Proc., § 410.10

- Directing solicitation or advertising to California residents could constitute “doing business” in California.
- Repeated and successive transactions in California, remotely and online, could constitute “doing business.”

So what does this mean for businesses trying to determine whether they need to comply with the CCPA? A thorough examination of the business’s activities and contacts – direct and indirect – within the State is necessary. If in doubt, companies should either assume compliance will be required, or anticipate that they may need to be able to document their lack of connections to California if they are named in a suit under the CCPA. For companies that believe that they are outside of the scope of the CCPA, but attempting to mitigate the risk of future lawsuits, it may be worth creating documentation which could be leveraged in litigation to explain the lack of California contacts.

FAQ. 3 DOES THE CCPA OPEN HEALTH CARE PROVIDERS TO INCREASED LITIGATION?

Probably not.

The CCPA exempts any health care provider or "covered entity" that is governed by the Health Insurance Portability and Accountability Act ("HIPAA"),[7] and it exempts "protected health information that is collected by a covered entity or business associate" subject to the HIPAA Security Rule.[8] Unlike the exemption provided to other industries (e.g., financial institutions), the exemption provided to health care providers, other covered entities, and business associates appears to cover all aspects of the CCPA, including the ability of a Californian to bring a private right of action or seek statutory damages following a data breach.

[7] CCPA, Section 1798.145(c)(1)(A).

[8] CCPA, Section 1798.145(c)(1)(B).

FAQ. 4 DOES THE CCPA OPEN FINANCIAL INSTITUTIONS TO INCREASED LITIGATION?

Yes.

While the CCPA provides a partial exemption for information collected by financial institutions that are subject to the Gramm Leach Bliley Act (e.g., information about individuals who have obtained personal financial products from the institution), that exemption does not apply to Section 1798.150 of the CCPA, which confers a private right of action on consumers to seek statutory damages against a business following a data security breach.[9] It is worth noting that the relatively narrow scope of the financial institution exemption within the CCPA contrasts with broader exemptions provided to financial institutions by other states. For example, the following compares the financial institution exemption provided in the CCPA with the broader exemption provided in Nevada's online privacy statute:

CCPA	**Nevada Online Privacy Notice Statute**
Statute does 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 . . . . This subdivision shall not apply to Section 1798.150 [the data breach right of action of the CCPA].[10]	Statute does not apply to "A financial institution or an affiliate of a financial institution that is subject to the provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq., and the regulations adopted pursuant thereto.[11]

[9] CCPA, Section 1798.145(e).

[10] CCPA, Section 1798.145(e) (emphasis added).

[11] Nevada Senate Bill 220 (Enacted May 29, 2019).

FAQ. 5 DOES THE CCPA OPEN INSURANCE COMPANIES TO INCREASED LITIGATION?

Yes.

The CCPA provides a partial exemption for information collected by financial institutions that are subject to the Gramm Leach Bliley Act (e.g., information about individuals who have obtained personal financial products from the institution). Insurance companies are generally considered "financial institutions" subject to the Gramm Leach Bliley Act, as well as any regulations imposed by state insurance commissioners pursuant to the Act. While the CCPA's financial institution exemption provides some protection to insurers, that exemption does not apply to Section 1798.150 of the CCPA which confers a private right of action on consumers to seek statutory damages against a business following a data security breach.[12] It is worth noting that the relatively narrow scope of the financial institution exemption within the CCPA contrasts with broader exemptions provided to financial institutions by other states. For example, the following compares the financial institution exemption provided in the CCPA with the broader exemption provided in Nevada's online privacy statute:

CCPA	**Nevada Online Privacy Notice Statute**
Statute does 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 . . . . This subdivision shall not apply to Section 1798.150 [the data breach right of action of the CCPA].[13]	Statute does not apply to "A financial institution or an affiliate of a financial institution that is subject to the provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq., and the regulations adopted pursuant thereto.[14]

[12] CCPA, Section 1798.145(e).

[13] CCPA, Section 1798.145(e) (emphasis added).

[14] Nevada Senate Bill 220 (Enacted May 29, 2019).

FAQ. 6 CAN A COMPANY BE SUED UNDER THE CCPA FOR FAILING TO POST A PRIVACY NOTICE?

No.

Section 1798.150 of the CCPA permits consumers to "institute a civil action" only where consumer "nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to unauthorized access and exfiltration, theft, or disclosure."[15] The CCPA does not provide a private right of action, nor does it provide statutory damages, if a company violates its obligations to provide notice concerning its privacy practices.[16]

It should be noted that the California Unfair Competition Law ("UCL") defines "unfair competition" as including "any unlawful, unfair, or fraudulent business act or practice."[17] Plaintiffs' attorneys in California have historically attempted to use the text of the UCL to bring suit against companies that allegedly violated any other California or federal law arguing that the secondary violation constituted an "unlawful" practice for which the UCL might permit recovery. It is unlikely, however, that such a strategy would succeed in connection with the CCPA, as the Act expressly 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."[18]

An amendment to the CCPA – Senate Bill 561 – was proposed which, if passed, would have extended the private right of action and the ability for plaintiffs' attorneys to seek statutory damages to all alleged violations of the CCPA. While the amendment received the endorsement of the California Attorney General, it failed to pass. However, it could come back for a vote at some point in the future.

The net result is that the CCPA, as it currently stands, will not permit consumers to sue businesses that fail to post a privacy notice, and it is unlikely that courts will permit such suits through the auspices of the UCL. The California legislature could, however, decide at any time to amend the CCPA to provide a private right of action.

[15] Cal. Civil Code 1798.150(a)(1).

[16] Cal. Civil Code 1798.100(b); 1798.110(c); 1798.115(c); 1798.130(a)(5). Note, however, that the CCPA does permit the California Attorney General to pursue civil penalties.

[17] Cal. Bus. & Prof. Code 17200.

[18] Cal. Civil Code 1798.150(c).

FAQ. 7 CAN A COMPANY BE SUED UNDER THE CCPA FOR FAILING TO HONOR AN ACCESS REQUEST?

No.

Section 1798.150 of the CCPA permits consumers to "institute a civil action" only where consumer "nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to unauthorized access and exfiltration, theft, or disclosure."[19] The CCPA does not provide a private right of action, nor does it provide statutory damages, if a company violates its obligations to disclose to consumers information about their data upon request, or provide "the specific pieces of personal information" collected about a consumer.[20]

The California Unfair Competition Law ("UCL") defines "unfair competition" as including "any unlawful, unfair, or fraudulent business act or practice."[21] Plaintiffs' attorneys in California have historically attempted to use the text of the UCL to bring suit against companies that allegedly violated any other California or federal law arguing that the secondary violation constituted an "unlawful" practice for which the UCL might permit recovery. It is unlikely, however, that such a strategy would succeed in connection with the CCPA as the Act expressly 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."[22]

An amendment to the CCPA – Senate Bill 561 – was proposed which, if passed, would have extended the private right of action and the ability for plaintiffs' attorneys to seek statutory damages to all alleged violations of the CCPA. While the amendment received the endorsement of the California Attorney General, it failed to pass. However, it could come back for a vote at some point in the future.

The net result is that the CCPA, as it currently stands, will not permit consumers to sue businesses that are alleged to have failed to honor access requests, and it is unlikely that courts will permit such suits through the auspices of the UCL. The California legislature could, however, decide at any time to amend the CCPA to provide a private right of action in connection with access requests.

[19] Cal. Civil Code 1798.150(a)(1).

[20] Cal. Civil Code 1798.100(a); 1798.110(a)(5). Note, however, that the CCPA permits the California Attorney General to pursue civil penalties.

[21] Cal. Bus. & Prof. Code 17200.

[22] Cal. Civil Code 1798.150(c).

FAQ. 8 CAN A COMPANY BE SUED UNDER THE CCPA FOR FAILING TO HONOR A DELETION REQUEST?

No.

Section 1798.150 of the CCPA permits consumers to "institute a civil action" only where consumer "nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to unauthorized access and exfiltration, theft, or disclosure."[23] The CCPA does not provide a private right of action, nor does it provide statutory damages, if a company violates its obligation to delete personal information about a consumer after receiving a deletion request.[24]

The California Unfair Competition Law ("UCL") defines "unfair competition" as including "any unlawful, unfair, or fraudulent business act or practice."[25] Plaintiffs' attorneys in California have historically attempted to use the text of the UCL to bring suit against companies that allegedly violated any other California or federal law arguing that the secondary violation constituted an "unlawful" practice for which the UCL might permit recovery. It is unlikely, however, that such a strategy would succeed in connection with the CCPA as the Act expressly 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."[26]

An amendment to the CCPA – Senate Bill 561 – was proposed which, if passed, would have extended the private right of action and the ability for plaintiffs' attorneys to seek statutory damages to all alleged violations of the CCPA. While the amendment received the endorsement of the California Attorney General, it failed to pass. However, it could come back for a vote at some point in the future.

The net result is that the CCPA, as it currently stands, will not permit consumers to sue businesses that are alleged to have failed to honor deletion requests, and it is unlikely that courts will permit such suits through the auspices of the UCL. The California legislature could, however, decide at any time to amend the CCPA to provide a private right of action in connection with deletion requests.

[23] Cal. Civil Code 1798.150(a)(1).

[24] Cal. Civil Code 1798.105(a). Note, however, that the CCPA permits the California Attorney General to pursue civil penalties.

[25] Cal. Bus. & Prof. Code 17200.

[26] Cal. Civil Code 1798.150(c).

FAQ. 9 CAN A COMPANY BE SUED UNDER THE CCPA FOR FAILING TO POST A "DO NOT SELL MY PERSONAL INFORMATION" LINK?

No.

Section 1798.150 of the CCPA permits consumers to "institute a civil action" only where consumer "nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to unauthorized access and exfiltration, theft, or disclosure."[27] The CCPA does not provide a private right of action, nor does it provide statutory damages, if a company violates its obligation to include a "do not sell my personal information" link on the company's homepage.[28]

The California Unfair Competition Law ("UCL") defines "unfair competition" as including "any unlawful, unfair, or fraudulent business act or practice."[29] Plaintiffs' attorneys in California have historically attempted to use the text of the UCL to bring suit against companies that allegedly violated any other California or federal law arguing that the secondary violation constituted an "unlawful" practice for which the UCL might permit recovery. It is unlikely, however, that such a strategy would succeed in connection with the CCPA as the Act expressly 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."[30]

An amendment to the CCPA – Senate Bill 561 – was proposed which, if passed, would have extended the private right of action and the ability for plaintiffs' attorneys to seek statutory damages to all alleged violations of the CCPA. While the amendment received the endorsement of the California Attorney General, it failed to pass. However, it could come back for a vote at some point in the future.

The net result is that the CCPA, as it currently stands, will not permit consumers to sue businesses that are alleged to have failed to include a "do not sell my personal information" link, and it is unlikely that courts will permit such suits through the auspices of the UCL. The California legislature could, however, decide at any time to amend the CCPA to provide a private right of action in connection with a failure to include the opt-out link on webpages.

[27] Cal. Civil Code 1798.150(a)(1).

[28] Cal. Civil Code 1798.135(a)(1). Note, however, that the CCPA permits the California Attorney General to pursue civil penalties.

[29] Cal. Bus. & Prof. Code 17200.

[30] Cal. Civil Code 1798.150(c).

FAQ. 10 CAN A COMPANY BE SUED UNDER THE CCPA FOR USING BEHAVIORAL ADVERTISING?

Many companies, such as online retailers and social media websites, participate in "behavioral advertising" networks. To participate in a behavioral advertising network, a company typically places code on its website that permits a third party (the behavioral advertising company) 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 visited. The third party behavioral advertising network then 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 network provider can discern characteristics about the consumer to help deliver targeted advertising.

The Law Before The CCPA*.* Before the CCPA was enacted, a company could be sued for using behavioral advertising if it failed to disclose to the consumer that it was collecting and disseminating the consumer's information to third-parties, or if its privacy policy otherwise misled the consumer into believing the information was not being shared. Plaintiffs have pursued such actions under the California Unfair Competition Law ("UCL") or the California Consumer Legal Remedies Act ("CLRA"). The biggest hurdle for plaintiffs in pursuing these actions was often establishing a monetary injury as a result of the dissemination of the information, in order to establish standing under either statute.

For example, in *In Re Facebook Privacy Litigation*, a class of Facebook users brought an action against Facebook for sharing their personal information with third-party advertisers without the users' knowledge or consent and in violation of Facebook's privacy policy. The Court dismissed both the UCL and CLRA claims with prejudice:

> To assert a UCL claim, a private plaintiff needs to have suffered injury in fact and . . . lost money or property as a result of the unfair competition. A plaintiff's 'personal information' does not constitute property under the UCL.
>
> Here, Plaintiffs do not allege that they lost money as a result of Defendant's conduct. Instead, Plaintiffs allege that Defendant unlawfully shared their 'personally identifiable information' with third-party advertisers. (Complaint ¶¶ 1–3.) However, personal information does not constitute property for purposes of a UCL claim.
>
> Plaintiffs do not allege that they paid fees for Defendant's services. Instead, they allege that they used Defendant's services 'free of charge.' (Complaint ¶ 12.) Because Plaintiffs allege that they

> received Defendant's services for free, as a matter of law, Plaintiffs cannot state a UCL claim under their own allegations.[31]

The Court dismissed the CLRA claim for similar reasons – finding plaintiffs did not qualify as "consumers" under that statute because they did not "'purchase [] or lease [] any goods or services,'" but instead, received Facebook's services for free.[32]

In contrast to the Facebook case, courts in California have upheld some UCL and CLRA claims alleging that plaintiffs did not consent to the sharing of their data with advertisers where the plaintiffs alleged (i) they paid for the goods or services used, and (ii) would have paid less for them had they known their information was being shared.

Thus, before the CCPA, a plaintiff (or group of plaintiffs) could allege state law claims related to behavioral advertising if they alleged: (1) the defendant failed to disclose or otherwise deceived the plaintiff(s) into believing their information would not be shared, and (2) the plaintiff suffered some monetary harm in connection with the purchase of a good or service.

The CCPA's Impact On Lawsuits Concerning Behavioral Advertising. 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."[33] The CCPA broadly defines the term "sell" as including the act of "disclosing" or "making available" personal information "for monetary or other valuable consideration."[34] "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."[35]

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. Specifically, the service provider exception requires that three conditions be present: First, the transfer of information to the service provider must be "necessary" for the website's business purpose.[36] While the facilitation of targeted advertising may be desirable, it is questionable whether

[31] *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 714–15 (N.D. Cal. 2011), *aff'd*, 572 F. App'x 494 (9th Cir. 2014) (citations and internal quotation marks omitted).

[32] *Id.* at 717.

[33] CCPA, Section 1798.130(A)(5)(C)(i).

[34] CCPA, Section 1798.140(t)(1).

[35] CCPA, Section 1798.140(o)(1)(A), (F).

[36] CCPA, Section 1798.140(t)(2)(C).

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."[37] 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, a plaintiffs' attorney could to argue that the contracts 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."[38] 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.
- *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.[39]

If the company fails to request consent or adequately disclose the sale of information, plaintiffs may seek to pursue causes of action against the company under the CCPA. However, the CCPA itself provides a private right of action only in the narrow circumstance of a data breach. Section 1798.150 provides for statutory damages where a "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 unauthorized access and exfiltration, theft, or disclosure." It does not provide for statutory damages for a company's failure to disclose that it shares a consumer's information with a third-party advertiser.

[37] CCPA, Section 1798.140(t)(2)(C)(ii), (v).

[38] CCPA, Section 1798.140(t)(2)(A).

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

Moreover, the statutory damages section expressly states: "Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law." In other words, while the CCPA provides stricter requirements on companies to disclose that they are disseminating users' information to third-parties, it does not itself appear to create a cause of action for failure to satisfy these requirements under the "unlawfulness" prong of the UCL or any other state law.[40]

Nevertheless, the CCPA makes clear that it does not "relieve any party from any duties or obligations imposed under other law or the United States or California Constitution."[41] Thus, the case law under the UCL and CLRA that pre-dates the CCPA remains good law.

The CCPA merely imposes additional restrictions on companies' privacy policies, while not relieving companies of any liability under the UCL or CLRA for failure to adequately implement such policies. To the extent that a class of plaintiffs can allege actual monetary harm (as a result of, for example, overpayment of a good or a service), then they might be able to continue to be able to bring UCL and CLRA causes of actions against companies that fail to properly disclose the transmission of consumers' information to third-parties for advertisement purposes. This is all the more reason for companies to either (i) request consent of a user before transmitting his or her information to advertisers; or (ii) disclose the transmittal as a "sale" of information and provide the opportunity to opt out.

Proposed Legislation Amending The CCPA. While the CCPA itself merely leaves existing law intact and does not itself create a private right of action for disseminating consumers' information to third-parties, proposed legislation sought to change this. An amendment to the CCPA – Senate Bill 561 – was proposed which, if passed, would have extended the private right of action and the ability for plaintiffs' attorneys to seek statutory damages to all alleged violations of the CCPA. While the amendment received the endorsement of the California Attorney General, it failed to pass. However, it could come back for a vote at some point in the future.

Conclusion. In sum, the CCPA, as enacted, provides additional restrictions on companies that use behavioral advertising, but does not provide a separate private action for plaintiffs to sue for violation of these restrictions. The CCPA also does not do away with current law under the UCL and CLRA. Those statutes might permit claims concerning behavioral advertising if a defendant failed to disclose or otherwise deceived a plaintiff into believing their information would not be shared, *and* the plaintiff suffered some monetary harm in connection with the purchase of a good or service. The California Attorney General has indicated

[40] *Id.*

[41] *Id.*

support for an amendment to the CCPA that would markedly change this landscape and provide an additional statutory basis to sue for violation of the CCPA's regulations concerning sale of information to third-parties. While that amendment failed in 2019, it is possible it will re-emerge in the future.

FAQ. 11 CAN A COMPANY BE SUED UNDER THE CCPA FOR FAILING TO PROTECT PERSONAL INFORMATION?

Yes.

Section 1798.150 of the CCPA permits consumers to "institute a civil action" if consumer "personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to unauthorized access and exfiltration, theft, or disclosure," and where that unauthorized access was "a result of the business's violation" of a duty to "implement and maintain reasonable security procedures and practices . . . ."[42] As a result there appear to be five elements necessary for a plaintiff to prove in order to successfully bring suit under the CCPA:

1. A business incurred a data breach;

2. The data breach involved a sensitive category of information identified in California Civil Code Section 1798.81.5;

3. The business had a legal duty to protect the personal information from breach;

4. The business failed to implement reasonable security procedures and practices; and

5. The business's failure resulted in (i.e., caused) the data breach.

[42] Cal. Civil Code 1798.150(a)(1).

FAQ. 12 DOES THE CCPA DEFINE “PERSONAL INFORMATION” DIFFERENTLY FOR PRIVACY AND SECURITY PURPOSES?

Yes.

The sections of the CCPA that relate to data privacy (i.e., the collection, use, and sharing of information) use a definition of “personal information” that includes approximately 26 categories or types of data.[43] In contrast, the sections of the CCPA that relate to data security (i.e., the protection of information) adopt a far narrower definition of “personal information” that includes only 6 categories of types of data. The following chart indicates which categories of personal information apply to the data privacy and the data security sections of the CCPA:

Examples of Personal Information	Applies to Privacy Requirements of CCPA	Applies to Security Requirements of CCPA
1. Audio, electronic, visual, thermal, olfactory, or similar information	✓[44]	
2. Bank account number	✓[45]	✓[46]
3. Biometric information	✓[47]	
4. Commercial information (e.g., products or services purchased, or other purchasing or consuming histories or tendencies)	✓[48]	
5. Credit card number	✓[49]	✓[50]
6. Debit card number	✓[51]	✓[52]
7. Driver’s License Number / State ID	✓[53]	✓[54]
8. Education	✓[55]	
9. Electronic network activity (e.g., browsing history)	✓[56]	
10. Email address	✓[57]	Partial ✓[58]

[43] CCPA, Section 1798.140(0)(1).

[44] 1798.140(o)(1)(H).

[45] 1798.80(e) (integrated via 1798.140(o)(B)).

[46] 1798.80(e) (integrated via 1798.140(o)(B)).

[47] 1798.140(o)(1)(E).

[48] 1798.140(o)(1)(D).

[49] 1798.80(e) (integrated via 1798.140(o)(B)).

[50] 1798.81.5(d)(1)(A)(iii) (in combination with name).

[51] 1798.80(e) (integrated via 1798.140(o)(B)).

[52] 1798.81.5(d)(1)(A)(iii) (in combination with name).

[53] 1798.80(e) (integrated via 1798.140(o)(B)).

[54] 1798.81.5(d)(1)(A)(ii) (in combination with name).

[55] 1798.140(o)(1)(J) (within the scope of FERPA).

[56] 1798.140(o)(1)(F).

[57] 1798.140(o)(1)(A).

[58] 1798.81.5(d)(1)(A)(ii) (only if the email address is in combination with a password).

Examples of Personal Information		Applies to Privacy Requirements of CCPA	Applies to Security Requirements of CCPA
11.	Employment	✓[59]	
12.	Employment history	✓[60]	
13.	Geolocation data	✓[61]	
14.	Health insurance information	✓[62]	✓[63]
15.	Identifiers (e.g., name or alias)	✓[64]	Partial ✓[65]
16.	Insurance Policy Number	✓[66]	✓[67]
17.	Medical information	✓[68]	✓[69]
18.	Online identifier (e.g. IP address)	✓[70]	
19.	Other financial information	✓[71]	
20.	Passport Number	✓[72]	
21.	Physical Characteristics	✓[73]	
22.	Postal address	✓[74]	
23.	Signature	✓[75]	
24.	Social Security Number	✓[76]	✓[77]
25.	Telephone Number	✓[78]	
26.	Transaction information	✓[79]	

[59] 1798.140(o)(1)(D).

[60] 1798.140(o)(1)(I).

[61] 1798.140(o)(1)(G).

[62] 1798.80(e) (integrated via 1798.140(o)(B)).

[63] 1798.81.5(d)(1)(A)(v) (in combination with name).

[64] 1798.140(o)(1)(A).

[65] 1798.81.5(d)(1)(A)(ii) (only if a name is in combination with another sensitive field, or if a username or email address is in combination with a password).

[66] 1798.80(e) (integrated via 1798.140(o)(B)).

[67] 1798.81.5(d)(1)(A)(iv) (in combination with name).

[68] 1798.80(e) (integrated via 1798.140(o)(B)).

[69] 1798.81.5(d)(1)(A)(iv) (in combination with name).

[70] 1798.140(o)(1)(A).

[71] 1798.80(e) (integrated via 1798.140(o)(B)).

[72] 1798.140(o)(1)(A).

[73] 1798.80(e) (integrated via 1798.140(o)(B)).

[74] 1798.140(o)(1)(A).

[75] 1798.80(e) (integrated via 1798.140(o)(B)).

[76] 1798.140(o)(1)(A).

[77] 1798.81.5(d)(1)(A)(i) (in combination with name).

[78] 1798.80(e) (integrated via 1798.140(o)(B)).

[79] 1798.140(o)(1)(D).

FAQ. 13 DOES THE CCPA ALLOW AN INDIVIDUAL WHOSE NAME IS COMPROMISED THROUGH A DATA BREACH TO SEEK STATUTORY DAMAGES?

No.

The Act generally defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[80] The Act includes a non-exhaustive list of examples of personal information which makes clear that "[i]dentifiers such as real name" falls within the definition.[81]

While "real name" falls within the general definition of "personal information," the section of the CCPA that permits consumers to bring suit to recover statutory damages following a data breach only applies to "nonencrypted or nonredacted personal information, *as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5* . . . ."[82] That subsection contains a much narrower definition of "personal information" that includes only the following data elements:

1. Name and Social security number;

2. Name and driver's license number or California identification card number;

3. Name and account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

4. Name and medical information;

5. Name and health insurance information;[83] or

6. A username or email address in combination with a password or security question and answer that would permit access to an online account.

[80] CCPA, Section 1798.140(o)(1).

[81] CCPA, Section 1798.140(o)(1)(A).

[82] CCPA, Section 1798.150(a)(1) (emphasis added).

[83] Cal. Civil. Code. Section 1798.81.5(d)(1)(A).

Thus, although the CCPA generally regulates the collection, sharing, and deletion of names, the statutory damages provision would not permit an individual whose name was the subject of unauthorized disclosure as a result of a data breach to initiate suit or to seek statutory damages unless the name was lost in combination with more sensitive data fields.

FAQ. 14 DOES THE CCPA ALLOW AN INDIVIDUAL WHOSE EMAIL ADDRESS IS COMPROMISED THROUGH A DATA BREACH TO SEEK STATUTORY DAMAGES?

No, not unless accompanied by a password that would give access to an online account.

The Act generally defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[84] The Act includes a non-exhaustive list of examples of personal information which makes clear that "email address" falls within the definition.[85]

While "email address" falls within the general definition of "personal information," the section of the CCPA that permits consumers to bring suit to recover statutory damages following a data breach only applies to "nonencrypted or nonredacted personal information, *as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5* . . . ."[86] That subsection contains a much narrower definition of "personal information" that includes only an individual's first name or first initial and his or her last name in combination with one of the following data elements:

1. Name and Social security number;

2. Name and driver's license number or California identification card number;

3. Name and account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

4. Name and medical information;

5. Name and health insurance information;[87] or

6. A username or email address in combination with a password or security question and answer that would permit access to an online account.

[84] CCPA, Section 1798.140 (o)(1).

[85] CCPA, Section 1798.140(o)(1)(A).

[86] CCPA, Section 1798.150(a)(1).

[87] Cal. Civil. Code. Section 1798.81.5(d)(1)(A).

Thus, although the CCPA generally regulates the collection, sharing, and deletion of email addresses, the statutory damages provision would not permit an individual whose email address alone was the subject of unauthorized disclosure as a result of a data breach to initiate suit or to seek statutory damages.

FAQ. 15 DOES THE CCPA ALLOW AN INDIVIDUAL WHOSE BUSINESS CONTACT INFORMATION IS COMPROMISED THROUGH A DATA BREACH TO SEEK STATUTORY DAMAGES?

No.

Section 1798.150(a)(1) allows "[a]ny 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 unauthorized access and exfiltration, theft, or disclosure" to recover statutory damages and other nonmonetary relief if they can show the access, exfiltration, theft, or disclosure resulted from the "business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information…."[88]

Elsewhere in the Act, "personal information" is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[89] The Act also provides a non-exhaustive list of examples of personal information which includes "employment,"[90] as well as "professional or employment-related information."[91]

The net result of this definition is that business contact information, such as the employee's name, job title, company, business address, work phone number, etc. are arguably covered within the definition of "personal information." In contrast, generic business names, business addresses, generic email addresses or any other general business information, as long as the information has not been linked to an individual, are arguably not covered within the definition. So, for example, "John.Smith@acme.com" would most likely be considered "personal information" governed generally by the CCPA whereas "contact@acme.com" would not, even if the latter is used by the same employee to communicate with the public.

In addition, an amendment to the Act carved out business contact information from the purview of the CCPA, at least until 2021. Such information alone would not give rise to a private cause of action if breached. The statutory damages provision relies upon a much narrower definition of "personal information" set forth in Civil Code Section 1798.81.5(d)(1)(A). That section states:

[88] CCPA, Section 1798.150(a)(1).

[89] CCPA, Section 1798.140 (o)(1).

[90] CCPA, Section 1798.140(o)(1)(B); California Civil Code 1798.80(e).

[91] CCPA, Section 1798.140(o)(1)(I).

> (1) "Personal information" means either of the following: (A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social security number. (ii) Driver's license number or California identification card number. (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv) Medical information. (v) Health insurance information.[92]

Thus, disclosure of a work email address or business contact information alone would be insufficient to state a claim under the CCPA's statutory damages provision.

[92] Cal. Civil. Code. 1798.81.5(d)(1)(A).

FAQ. 16 DOES THE CCPA ALLOW AN INDIVIDUAL WHOSE IP ADDRESS IS COMPROMISED THROUGH A DATA BREACH TO SEEK STATUTORY DAMAGES?

No.

Section 1798.150(a)(1) allows "[a]ny 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 unauthorized access and exfiltration, theft, or disclosure" to recover statutory damages and other nonmonetary relief if they can show the access, exfiltration, theft, or disclosure resulted from the "business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information…."[93]

Elsewhere in the Act, "personal information" is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[94] While the Act provides a list of examples of personal information – which explicitly includes "Internet Protocol Address" – it qualifies the examples by stating that they only fall within the definition of personal information *if* they identify, relate to, describe, are "capable of being associated with," or "could reasonably be linked" with a particular person.[95]

While the Act generally includes IP addresses within the definition of "personal information," the statutory damages provision relies upon the much narrower definition of "personal information" set forth in Civil Code section 1798.81.5(d)(1)(A). That section states:

> (1) "Personal information" means either of the following: (A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social security number. (ii) Driver's license number or California identification card number. (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv) Medical information. (v) Health insurance information.[96]

[93] CCPA, Section 1798.150(a)(1).

[94] CCPA, Section 1798.140(o)(1).

[95] CCPA, Section 1798.140(o)(1).

[96] Cal. Civil. Code. 1798.81.5(d)(1)(A).

Thus, although the CCPA may generally regulate the privacy of consumers' IP addresses, the statutory damages provision appears to expressly exclude a cause of action based on unauthorized access, exfiltration, theft, or disclosure of an IP address.

FAQ. 17 WHAT CATEGORIES OF INFORMATION COULD TRIGGER A CONSUMER CLASS ACTION IF BREACHED?

Consumers can successfully bring suit under the CCPA if they can prove the following five elements:

1. A business incurred a data breach;

2. The data breach involved a sensitive category of information identified in California Civil Code Section 1798.81.5;

3. The business had a legal duty to protect the personal information from breach;

4. The business failed to implement reasonable security procedures and practices; and

5. The business's failure resulted in (i.e., caused) the data breach.

The definition of personal information used in California Civil Code Section 1798.81.5 is far narrower than the definition of personal information used within the rest of the CCPA. Specifically while the CCPA's general definition of 'personal information' contains 26 examples of types of data fields, only the following six data combinations can form the basis of a consumer lawsuit:

1. Name and social security number;

2. Name and driver's license number or California identification card number;

3. Name and account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

4. Name and medical information;

5. Name and health insurance information.

6. A username or email address in combination with a password or security question and answer that would permit access to an online account.[97]

[97] Cal. Civil. Code 1798.81.5(d)91)(A)

FAQ. 18 CAN EMPLOYEES BRING A CLASS ACTION UNDER THE CCPA FOLLOWING A DATA BREACH?

More than likely.

"Consumers" can bring suit under the CCPA if they can prove the following five elements:

1. A business incurred a data breach;
2. The data breach involved a sensitive category of information identified in Cal. Civil Code Section 1798.81.5;
3. The business had a legal duty to protect the personal information from breach;
4. The business failed to implement reasonable security procedures and practices; and
5. The business's failure resulted in (i.e., caused) a data breach.

While the common definition of "consumer" suggests that it refers to an individual that has "consumed" a product or a service in relation to a company, the definition ascribed by the CCPA is far broader. The term is defined to include any "natural person who is a California resident."[98] Read literally, the phrase includes not only an individual that consumes a product (e.g., a customer of a store), but also that store's California-based employees, and California-based business contacts or prospective customers.

The CCPA was amended to delay the application of the CCPA to employees' and job applicants' personal information with respect to privacy rights (i.e., right of access and deletion) until January 1, 2021, but not exempt employees altogether.[99] Specifically, employees still are likely to be able to bring suit following a data breach if their sensitive personal information is exposed.

[98] CCPA, Section 1798.140(g).

[99] *See* Assembly Bill 25.

FAQ. 19 CAN NON-CALIFORNIA RESIDENTS BRING A CLASS ACTION UNDER THE CCPA FOLLOWING A DATA BREACH?

No.

"Consumers" can bring suit under the CCPA if they can prove the following five elements:

1. A business incurred a data breach;
2. The data breach involved a sensitive category of information identified in Cal. Civil Code Section 1798.81.5;
3. The business had a legal duty to protect the personal information from breach;
4. The business failed to implement reasonable security procedures and practices; and
5. The business's failure resulted in (i.e., caused) a data breach.

While the common definition of "consumer" suggests that it refers to an individual that has "consumed" a product or a service in relation to a company, the definition ascribed by the CCPA is that a "consumer" is any "natural person who is a California resident."[100] As a result, individuals that are not residents of California are not permitted to bring suit under the statute. As a practical matter, plaintiffs' counsel may also bring claims based upon common-law theories on behalf of non-California residents arising from the same breach. These plaintiffs, however, would not be entitled to recover statutory damages under the CCPA.

[100] CCPA, Section 1798.140(g) (emphasis added).

FAQ. 20 ARE BUSINESSES STRICTLY LIABLE IF A DATA BREACH OCCURS?

No.

The CCPA permits consumers to bring suit if a data breach occurs that was "a result of" the business failing to "implement and maintain reasonable security procedures and practices . . . ." Accordingly, strict liability should not attach simply because a data breach occurs. Put differently, a plaintiff must prove both that the breach was a result of a failure of the business's security procedures and practices, which were not reasonable given a number of factors. Such factors include the type of data that the business collected (i.e., the level of sensitivity of the data), the industry segment in which the business operates, the size of the business, and the type of breach that occurred.

FAQ. 21 IS A BUSINESS REQUIRED TO IMPLEMENT A WRITTEN INFORMATION SECURITY PLAN ("WISP") UNDER THE CCPA?

Not technically. While the CCPA provides for a statutory damages to California residents whose sensitive information is exposed in a data security breach, it does not expressly require a company to have a Written Information Security Plan ("WISP"). However, a plaintiff pursuing statutory damages under the CCPA will need to prove that a company failed to implement and maintain reasonable and appropriate data security procedures and practices.[101] In defending such a claim, it will be essential for a company to be able to identify such measures, which will generally be documented in a WISP.

In February 2016, California published the California Data Breach Report, in which it specifically identified the 20 controls set forth in the Center for Internet Security's Critical Security Controls ("CIS") as the "minimum level of security" an organization should meet.[102] Indeed, the report states that the "failure to implement all of the Controls that apply to an organization's environment constitutes a lack of reasonable security."

The format and contents of a WISP can greatly vary depending on an organization's operations. At a minimum, the organization's WISP should include a description of the following:

- The administrative safeguards that exist to keep sensitive personal information secure;
- The technical safeguards that exist to keep sensitive personal information secure;
- The physical safeguards that exist to keep sensitive personal information secure;
- The process used by the organization to identify, on a periodic basis, internal and external risks to the information that it maintains;
- The specific employee who is ultimately responsible for maintaining and implementing security policies;
- The sensitive information maintained by the organization;
- Where and how sensitive information will be stored within the organization;
- How sensitive information can be transported away from the organization;

[101] Pursuant to Cal. Civil Code 1798.81.5(b) a business that owns, licenses, or maintains sensitive categories of personal information must "implement and maintain reasonable security procedures and practices."

[102] Available at http://src.bna.com/cFY

- Procedures that discuss the following:
    - Username assignment
    - Password assignment
    - Encryption format
    - Provisioning of user credentials
    - De-provisioning of user credentials (e.g., for terminated employees)
    - Employee training on security topics
    - Destroying data
    - Retaining service providers that will have access to data

FAQ. 22 IS A BUSINESS REQUIRED TO IMPLEMENT A DATA BREACH INCIDENT RESPONSE PLAN ("IRP")?

No.

While the CCPA provides for a statutory damages to California residents whose sensitive information is exposed in a data security breach, it does not expressly require a company to have a Data Breach Incident Response Plan ("IRP"). An IRP explains how an organization handles security incidents. Among other things, the plan helps employees from different departments understand the role that they are expected to play when investigating a security incident and identifies other people within the organization with whom they should be coordinating. The plan also can help educate employees concerning what they should and should not do when faced with a security incident and can provide them with a reference guide for resources that may help them effectively respond to an incident or breach.

Although an organization is not required to have an IRP in place, a plaintiff pursuing statutory damages under the CCPA will need to prove that a company failed to implement and maintain reasonable and appropriate data security procedures and practices. In defending such a claim, it will be essential for a company to be able to identify such measures. An IRP will be helpful in establishing that the company took data security seriously and created a plan to quickly respond to a breach.

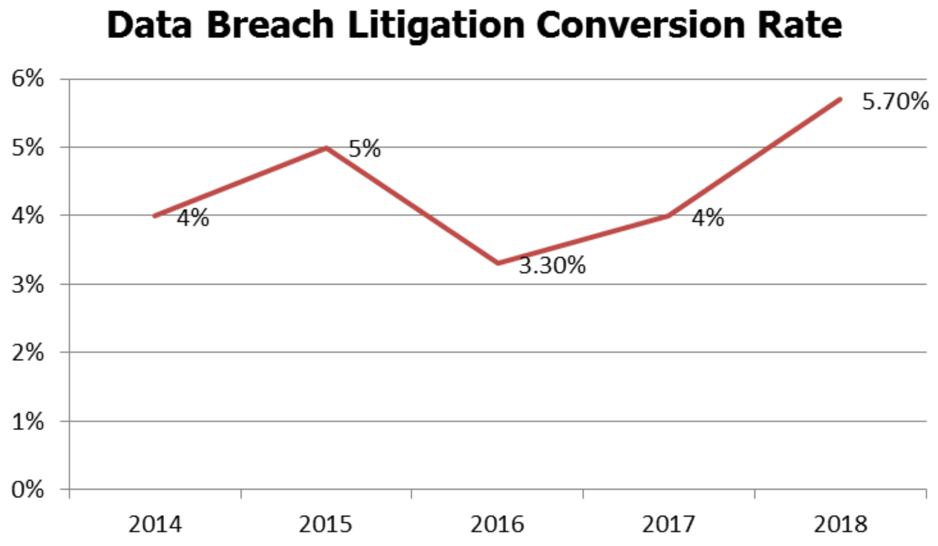
In February 2016, California published the California Data Breach Report, in which it specifically identified the 20 controls set forth in the Center for Internet Security's Critical Security Controls ("CIS") as the "minimum level of security" an organization should meet.[103] Indeed, the report states that the "failure to implement all of the Controls that apply to an organization's environment constitutes a lack of reasonable security." Number 19 on the CIS Critical Security Controls is "Incident Response and Management." Thus, having an IRP will provide useful evidence to establish the company complied with CIS.

[103] Available at http://src.bna.com/cFY

FAQ. 23 WHAT PERCENTAGE OF DATA BREACHES RESULT IN CLASS ACTION LITIGATION?

Around 5%.

For the last five years, BCLP has published the data security industry's leading analysis of data breach class action litigation.[104] As part of that study, BCLP reviews every class action complaint that is filed in a federal court against a private entity and that alleges recovery based upon a data security breach. BCLP also reviews all public data breaches reported by a third party tracking company. Using those data points, BCLP calculates a data breach litigation conversion rate – i.e., the percentage of publicly reported data breaches that turn into federal class action litigation. The data breach litigation conversion rate has been relatively consistent fluctuating between 3.3% and 5.7%:



It should be noted that the data breach litigation conversion rate does not account for state court litigation that was not removed to federal court.[105]

Despite the historical stability of the data breach litigation conversion rate, BCLP anticipates a significant increase in 2020 as a result of the ability of plaintiffs' attorneys to seek statutory damages under the CCPA.

[104] *See* 2019 Data Breach Litigation Report *available at* https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf.

[105] BCLP excluded state court litigation as state courts are inconsistent in their publication of filed complaints such that the inclusion of state-filed complaints that were not removed to federal court would inadvertently over-represent or under-represent the quantity of filings in any state as compared to the overall universe of class action filings.

FAQ. 24 CAN A PLAINTIFF CHOOSE TO FILE A CCPA CASE IN STATE COURT OR FEDERAL COURT?

It depends upon the facts involved in a specific breach.

The CCPA does not expressly prescribe that civil actions must be brought in state or federal court. As a result, if a party can establish that the jurisdictional requirements are met, the case may be brought in federal court or removed from state court to federal court. Specifically, federal courts are empowered to hear any case in which the plaintiff and defendant are citizens of different states (e.g., a California resident suing a company whose principal place of business and/or state of incorporation is in Utah) and where the amount in controversy is greater than $75,000. Under the CCPA, unless a particular plaintiff's actual damages are significant, this jurisdictional threshold is unlikely to be met, and a federal court would not be empowered to hear the matter.

The Class Action Fairness Act ("CAFA") provides another mechanism for federal court jurisdiction in class actions. If a representative plaintiff can establish that at least one defendant and one plaintiff are citizens of different states and the combined amount in controversy is greater than $5 million, then the action may be brought in, or removed to, federal court. The CCPA expressly contemplates that class actions may be brought after a data security breach, and it provides for statutory penalties of a minimum of $100 and a maximum of $750. If the class of California residents impacted is large enough (e.g., several thousand people), then it may be relatively easy to assert CAFA jurisdiction in federal court.

FAQ. 25 CAN A COMPANY REMOVE A CCPA CASE FILED IN CALIFORNIA STATE COURT TO A CALIFORNIA FEDERAL COURT?

It depends. The CCPA does not expressly prescribe that civil actions must be brought in state or federal court. However, defendant companies may find California federal courts to be more advantageous venues and therefore they may look to remove cases filed in state court to a federal court. A removing defendant has to establish from the face of the Complaint, however, that the jurisdictional requirements are met. Specifically, federal courts are empowered to hear any case in which the plaintiff and defendant are citizens of different states (e.g., a California resident suing a company whose principal place of business and/or state of incorporation is in Utah) where the amount in controversy is greater than $75,000. Under the CCPA, unless the plaintiff's actual damages are significant, this jurisdictional threshold is unlikely to be met, and a federal court would not have authority to hear the matter.

The Class Action Fairness Act ("CAFA") provides another mechanism for defendants to remove class actions to federal court. If a representative plaintiff is a citizen of a different state from at least one defendant and the combined amount in controversy is greater than $5 million, then the action may be removed to federal court. The CCPA expressly contemplates that class actions may be brought after a data security breach, and it provides for statutory penalties of a minimum of $100 and a maximum of $750. If the class of California residents impacted is large enough (e.g., several thousand people), then it may be relatively easy for a defendant to assert CAFA jurisdiction in federal court.

The right to remove is not absolute, however. Defendants still must remove the action within 30 days of an event triggering possible federal jurisdiction. In most instances, that will occur within 30 days of being served with the Complaint.

FAQ. 26 DOES A CONSUMER HAVE TO ESTABLISH INJURY TO BRING SUIT IN FEDERAL COURT IN CALIFORNIA UNDER THE CCPA?

Yes.

Section 1798.150 of the CCPA permits consumers to "institute a civil action" if the consumer's "personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to unauthorized access and exfiltration, theft, or disclosure," and where that unauthorized access was "a result of the business's violation" of a duty to "implement and maintain reasonable security procedures and practices …"[1]

However, a plaintiff suing in federal court must establish she has standing under Article III of the U.S. Constitution. Article III standing requires (1) an injury-in-fact, (2) fairly traceable to the challenged conduct, (3) that is likely to be redressed by a favorable judgment. The U.S. Supreme Court has held that the alleged of a statutory right does not automatically satisfy the injury-in-fact requirement just because a statute authorizes a person to sue to vindicate that right. Rather, to constitute an injury-in-fact, plaintiff's injury must be both concrete and particularized, and these requirements are to be evaluated separately, even when the plaintiff asserts a statutory violation. Concrete injuries can be tangible or intangible, but when the injury is intangible, the mere fact that a cause of action exists in law does not confer Article III standing. Instead, the intangible injury must be real and have a close relationship to traditional, common law harms.[2]

A consumer whose personal information is subject to a data breach but who has not been injured at all by the data breach – for example, where the consumer has not suffered actual fraud and cannot establish a substantial likelihood of future identity theft – cannot establish she meets the standing requirements of Article III and will not be able to pursue her claim in federal court. On the other hand, the standard of pleading required to establish injury-in-fact may be quite low; for example, if a consumer alleges she suffered anxiety resulting from unauthorized access to her data, or that she spent time freezing her credit and reviewing her credit reports, some federal courts may consider that sufficient to establish standing.

[1] Cal. Civil Code 1798.150(a)(1).

[2] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

FAQ. 27 CAN A CONSUMER BRING SUIT IN A CALIFORNIA STATE COURT THE CCPA EVEN IF THEY WERE NOT INJURED BY A DATA BREACH?

Yes, if they satisfy the elements of a CCPA data breach claim.

Section 1798.150 of the CCPA permits consumers to "institute a civil action" if the consumer's "personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to unauthorized access and exfiltration, theft, or disclosure," and where that unauthorized access was "a result of the business's violation" of a duty to "implement and maintain reasonable security procedures and practices …"

As a result, there appear to be five elements necessary to establish a claim under the CCPA:

1. A business incurred a data breach;
2. The data breach involved a sensitive category of information identified in Cal. Civil Code Section 1798.81.5;
3. The business had a legal duty to protect the personal information from breach;
4. The business failed to implement reasonable security procedures and practices; and
5. The business's failure resulted in (i.e., caused) the data breach.

Absent from these elements is a requirement that the affected consumer have suffered any injury as a result of the data breach. In fact, the CCPA provides that an affected consumer may recover "damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty [dollars] ($750) per consumer per incident or actual damages, whichever is greater."[106] (emphasis added.) And unlike Article III of the U.S. Constitution, which requires a plaintiff to establish standing to bring suit, the California Constitution empowers state courts to adjudicate any "cause" brought before them.[107] As a result, a consumer whose personal information was subject to a data breach (and who meets the other elements set forth above) may bring suit in California state court even if they were not injured by the data breach.

[106] Cal. Civil Code § 1798.150(a)(1)(A).

[107] Cal. Const., art. VI, § 10.

FAQ. 28 IN WHAT LOCATIONS CAN A PLAINTIFF FILE A CCPA CASE?

Litigants seeking a venue to file a data breach lawsuit under the CCPA typically must do so in a state or federal court with some tie to the events alleged in the complaint. In most instances, venue will be proper if the court sits in a location where the company the plaintiff is suing does business. However, a plaintiff may be able to establish that venue is proper in a location where the dispute arose. Although this may be more challenging to establish in a breach scenario, it is conceivable that a plaintiff may be able to assert that the location where they purchased a product or service that required them to provide their personal information to a company is an appropriate venue.

In federal court, if a plaintiff can establish neither of these, venue is appropriate in any location in which the court has personal jurisdiction over the defendant company. Typically, that will be where the company is headquartered or where the company has directed its activities so substantially that it should not be surprised to find itself the subject of a lawsuit in that location.

FAQ. 29 WHAT LEGAL THEORY ARE PLAINTIFFS MOST LIKELY TO ASSERT IN A DATA BREACH CLASS ACTION IN ADDITION TO THE CCPA?

Negligence.

For the last five years, BCLP has published the leading analysis of data breach class action litigation.[108] As part of that study, BCLP has reviewed every data breach class action complaint against a private company filed in (or removed to) federal court.[109] Among other variables, BCLP tracks the legal theories asserted by plaintiffs in data breach litigation.

As our 2019 Data Breach Litigation Report indicates, the most popular legal theory utilized by plaintiffs in data breach class action litigation is negligence. Indeed, while 47% of data breach class actions complaints asserted negligence as the primary (or only) legal theory, an additional 45% of data breach class action complaints asserted negligence as a secondary, or alternative, legal theory. As a result, 92% of data breach class action complaints alleged negligence as a legal theory of recovery.[110]

BCLP anticipates that in 2020, the most popular legal theory will shift from negligence to the CCPA as plaintiffs attempt to pursue the statutory damages referenced within Section 1798.150 of the Act. While the CCPA may become the most popular legal theory asserted by California residents, based upon historical trends, plaintiffs are likely to continue to allege additional legal theories including negligence. This is particularly true for claims asserted on behalf of non-California residents whose sensitive personal information is exposed in the same data breach, but who are not able to recover statutory damages under the CCPA.

[108] *See* 2019 Data Breach Litigation Report *available at* https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf.

[109] *See* 2019 Data Breach Litigation Report *available at* https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf. Note that the 2019 Data Breach Litigation Report excludes state court litigation as state courts are inconsistent in their publication of filed complaints and, as a result, inclusion of state-filed complaints that were not removed to federal court would inadvertently over-represent or under-represent the quantity of filings in any state depending upon whether a particular state (or a particular court) publishes electronic versions of case filings.

[110] *See* 2019 Data Breach Litigation Report at 14, 17 *available at* https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf.

FAQ. 30 WHAT OTHER LEGAL THEORIES COULD A PLAINTIFF ASSERT IN A DATA BREACH CLASS ACTION IN ADDITION TO THE CCPA?

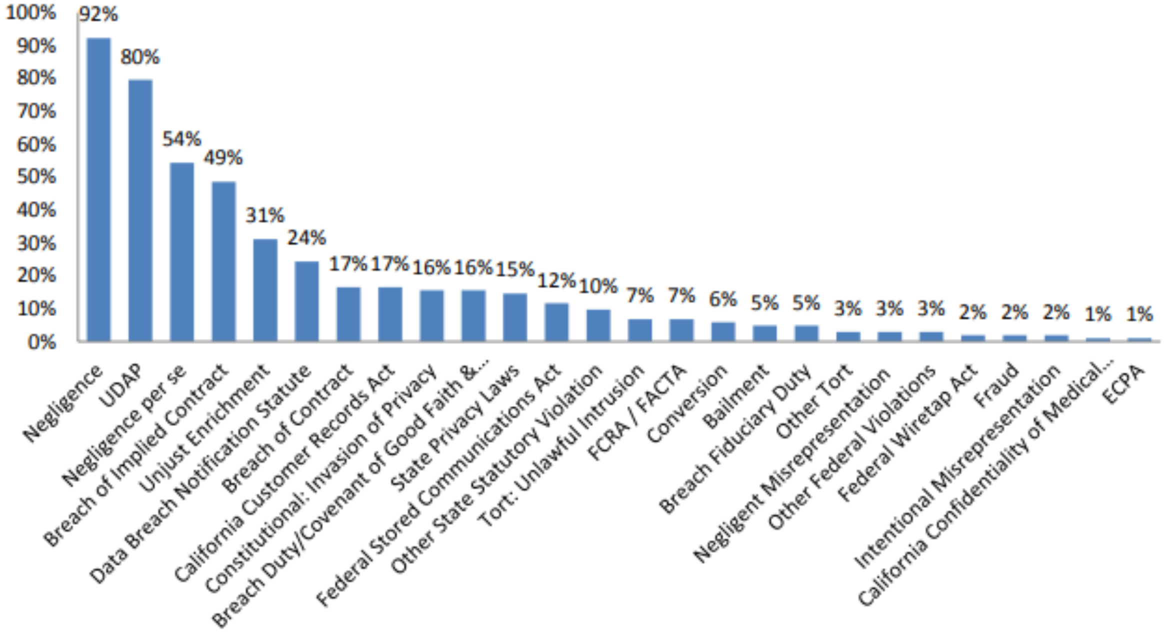
For the last five years, BCLP has published the leading study of data breach class action litigation.[111] As part of that study, BCLP has reviewed every data breach class action complaint against a private company filed in (or removed to) federal court.[112] Among other variables, BCLP tracked the legal theories asserted by plaintiffs in data breach litigation.

As our 2019 Data Breach Litigation Report indicates, plaintiffs asserted more than 25 legal theories in their attempts to recover against companies following data breaches. While the most popular legal theories focused on negligence, state unfair and deceptive trade practice laws, or the alleged breach of an implied contract, the variety of counts included in complaints demonstrates the creativity of the plaintiffs' bar as they have struggled to identify legal theories that could withstand judicial challenge:[113]

[111] *See* 2019 Data Breach Litigation Report *available at* https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf.

[112] *See* 2019 Data Breach Litigation Report *available at* https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf. Note that the 2019 Data Breach Litigation Report excludes state court litigation as state courts are inconsistent in their publication of filed complaints and, as a result, inclusion of state-filed complaints that were not removed to federal court would inadvertently over-represent or under-represent the quantity of filings in any state depending upon whether a particular state (or a particular court) publishes electronic versions of case filings.

[113] *See* 2019 Data Breach Litigation Report at 17 *available at* https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf.



While BCLP anticipates that in 2020 plaintiffs will congregate around the CCPA in an attempt to pursue the statutory damages referenced within Section 1798.150, plaintiffs are likely to continue to experiment with the legal theories identified above as alternative or supplementary sources of liability with regard to Californians, or as primary sources of liability with regard to residents of other states.

FAQ. 31 WHAT IS THE MOST POPULAR COURT FOR FILING DATA BREACH CLASS ACTIONS?

The United States District Court for the Central District of California.

For the last five years, BCLP has published the leading analysis of data breach class action litigation.[114] As part of that study, BCLP has reviewed every data breach class action complaint against a private company filed in federal court.[115] Among other variables, BCLP tracks the federal court in which a data breach class action has been filed (or the federal court to which a data breach class action is removed from state court). As our 2019 Data Breach Litigation Report indicates, the most popular forum for filing a data breach class action is the United States District Court for the Central District of California. Indeed, more than 1 out of every 4 data breach class actions was filed in that forum (26%). The second most popular forum for filing a data breach class action was the Northern District of California (13%). Combined, California district courts accounted for nearly half of all data breach class action filings.

While plaintiffs are not required to file a CCPA suit in a California court, BCLP anticipates that the enactment of the CCPA will further strengthen plaintiffs' attorneys' preference for filing suit in California courts.

[114] *See* 2019 Data Breach Litigation Report *available at* https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf.

[115] *See* 2019 Data Breach Litigation Report *available at* https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf. Note that the 2019 Data Breach Litigation Report excludes state court litigation as state courts are inconsistent in their publication of filed complaints and, as a result, inclusion of state-filed complaints that were not removed to federal court would inadvertently over-represent or under-represent the quantity of filings in any state depending upon whether a particular state (or a particular court) publishes electronic versions of case filings.

FAQ. 32 DO BUSINESSES HAVE TO REPORT DATA BREACHES TO THE STATE OF CALIFORNIA?

Sometimes.

While the CCPA does not require that companies report data breaches to the state of California, a 2012 amendment to California's data breach notification statute, originally enacted in 2003, requires that some data breaches that involve certain sensitive categories of information, such as Social Security Numbers, driver's license numbers, financial account numbers, medical information, or health insurance information, be reported to the California Attorney General if information of more than 500 California residents is impacted.[116] The Attorney General then posts a list of companies who have reported breaches on its website, which is publicly available.

[116] Cal. Civil Code 1798.82(f).

FAQ. 33 ONCE A DATA BREACH IS REPORTED TO THE STATE OF CALIFORNIA, IS IT POSTED TO A WEBSITE?

Yes.

The Office of the Attorney General publicly posts each data breach that is reported to its office on the following website: https://oag.ca.gov/privacy/databreach/list. Among other things, the attorney general includes the following information about each breach:

- The date that the data breach occurred;
- The date that the breach was reported to the Office of the Attorney General;
- The type of information impacted by the breach;
- A description of the factual situation that caused the breach; and
- A description of the actions taken by the impacted company.

FAQ. 34 CAN PLAINTIFFS' ATTORNEYS SEARCH AN ONLINE WEBSITE TO FIND THE NAMES OF EACH COMPANY THAT REPORTS A DATA BREACH IN CALIFORNIA?

Yes.

The California Office of the Attorney General posts each data breach that is reported to its office on the following website: https://oag.ca.gov/privacy/databreach/list. The website is publicly available and can not only be searched and sorted, but plaintiffs' attorneys also can download the following information about each breach:

- The date that the data breach occurred;
- The date that the breach was reported to the Office of the Attorney General;
- The type of information impacted by the breach;
- A description of the factual situation that caused the breach; and
- A description of the actions taken by the impacted company.

In light of the statutory damages referenced within Section 1798.150 of the CCPA, BCLP anticipates that beginning on January 1, 2020, plaintiffs' attorneys will use the information posted by the Office of the Attorney General as a roadmap to identify potential data breach class action defendants to target in class action complaints.

FAQ. 35 WHAT ARE "REASONABLE SECURITY PROCEDURES AND PRACTICES" UNDER THE CCPA?

Under the CCPA's private right of action, any consumer whose sensitive personal information has been compromised in a data breach can sue to recover hefty statutory damages of up to $750 "per customer per incident or actual damages, whichever is greater."[117] Consumers need to prove that the breach resulted from the organization's failure to "implement and maintain *reasonable* security procedures and practices appropriate to the nature of the information..."[118] Historically elusive, the definition of "reasonable security procedures and practices" is coming into focus.

On February 25, 2016, the Office of the California Attorney General released its 2016 California Data Breach Report, a study of the data breaches reported to the AG from 2012-2015. The Report, though now several years old, offers insights into how the Attorney General's office may exercise its enforcement powers under the CCPA and what factors the trier of fact may consider in deciding the "reasonableness" of an organization's data security procedures.

Most significant is the Attorney General's position that the Center for Internet Security's Critical Security Controls ("Controls"), a set of 20 cybersecurity defensive measures, "define a minimum level of information security that all organizations that collect or maintain personal information should meet," and that "[t]he failure to implement all the Controls that apply to an organization's environment" would "constitute[] a lack of reasonable security." In other words, the Controls may represent the baseline for what the Office of the Attorney General considers to be "reasonable security procedures and practices."

Notably, the Breach Report does not create any regulatory obligations, and it is uncertain whether it would be given the same weight by a court as an Attorney General advisory opinion,[119] but it strongly suggests that an organization's security procedures will be benchmarked against the Controls, and/or other well-accepted industry frameworks (*e.g.,* ISO 27002, NIST). In order to be best prepared to meet the "reasonableness" standard under the CCPA, organizations should consider a gap analysis of their information security practices against the Controls or comparable security frameworks, and a decision to adopt, or not to adopt, the Controls should be well documented and reasoned.

[117] CCPA, Section 1798.150(a)(1).

[118] *Id.* (emphasis supplied).

[119] *California Building Industry Association v. State Water Resources Control Board*, 8 Cal. App. 5th 52 (Ct. App. 2017) (Opinions of the Attorney General, while not binding upon courts, are entitled to great weight).

FAQ. 36 DOES THE CCPA SUGGEST A MINIMUM STATUTORY DAMAGE THAT A COURT SHOULD AWARD?

Yes.

Section 1798.150 of the CCPA permits consumers to "institute a civil action" if consumer "personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to unauthorized access and exfiltration, theft, or disclosure," and where that unauthorized access was "a result of the business's violation" of a duty to "implement and maintain reasonable security procedures and practices . . . ."[120] If a plaintiff is successful in bringing such a suit, the CCPA states that the plaintiff can recover "damages in an amount <u>not less than</u> one hundred dollars ($100) . . . per consumer per incident. . . ."[121]

[120] Cal. Civil Code 1798.150(a)(1).

[121] Cal. Civil Code 1798.150(a)(1)(A).

FAQ. 37 DOES THE CCPA IDENTIFY A MAXIMUM STATUTORY DAMAGE THAT CAN BE AWARDED?

Yes.

Section 1798.150 of the CCPA permits consumers to "institute a civil action" if consumer "personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to unauthorized access and exfiltration, theft, or disclosure," and where that unauthorized access was "a result of the business's violation" of a duty to "implement and maintain reasonable security procedures and practices . . . ."[122] If a plaintiff is successful in bringing such a suit, the CCPA states that the plaintiff can recover "damages in an amount . . . not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater."[123]

[122] Cal. Civil Code 1798.150(a)(1).

[123] Cal. Civil Code 1798.150(a)(1)(A).

FAQ. 38 WHAT FACTORS WILL COURTS LOOK TO WHEN DETERMINING WHAT STATUTORY DAMAGES TO AWARD?

Section 1798.150 of the CCPA permits consumers to "institute a civil action" if consumer "personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to unauthorized access and exfiltration, theft, or disclosure," and where that unauthorized access was "a result of the business's violation" of a duty to "implement and maintain reasonable security procedures and practices . . . ."[124] If a plaintiff is successful in bringing such a suit, the statute instructs a court to examine some, or all, of the following factors when determining the statutory damages to which the plaintiff may be entitled:

- Nature of the misconduct;
- Seriousness of the misconduct;
- Number of violations;
- Persistence of the misconduct;
- Length of time over which the misconduct occurred;
- Willfulness of the defendant's misconduct; and
- Defendant's assets, liabilities, and net worth.[125]

[124] Cal. Civil Code 1798.150(a)(1).

[125] Cal. Civil Code 1798.150(a)(2).

FAQ. 39 DOES A BUSINESS HAVE AN ABILITY TO "CURE" A SECURITY DEFICIENCY PRIOR TO STATUTORY DAMAGES BEING AWARDED?

Yes, although doing so may be difficult.

Before filing a lawsuit under the CCPA arising from a data security breach, a plaintiff seeking statutory damages must provide a business 30 days written notice identifying the specific provisions of the CCPA the plaintiff alleges have been, or are being, violated. The CCPA provides that "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."

Practically speaking, if a company has already suffered a data breach, certainly it would try to establish that it "cured" the root cause of the breach by, for example, patching a hole in software or implementing multi-factor authentication to prevent future access to a breached account. However, companies can expect that plaintiffs will argue that those efforts are insufficient and also would not "cure" the harm flowing from a breach – e.g., the risk of identity theft to the individuals. Thus, it is likely that businesses attempting to insulate themselves from lawsuits by explaining they "cured" the deficiency that lead to the breach will end up litigating those measures in court.

FAQ. 40 WHAT DOES IT MEAN TO “CURE” A SECURITY DEFICIENCY AFTER A BREACH HAS OCCURRED?

Before filing a lawsuit under the CCPA arising from a data security breach, a plaintiff seeking statutory damages must provide a business 30 days written notice identifying the specific provisions of the CCPA the plaintiff alleges have been, or are being, violated. The CCPA provides that “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.”

In a breach lawsuit, the complained of provision of the CCPA is almost certainly going to be the requirement that companies “implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.” Thus, a company that suffered a data breach should be prepared to implement measures to establish that the root cause of the breach has been addressed in a way that would prevent a similar breach from occurring again. For example, in a breach where a business email account was compromised, the company may try to cure by implementing multi-factor authentication.

Companies can expect that plaintiffs will file lawsuits notwithstanding efforts to cure. Plaintiffs will likely argue that the company’s efforts are insufficient and also would not “cure” the harm flowing from a breach – e.g., the risk of identity theft to the individuals. It will be left to the courts to determine what constitutes a sufficient “cure” under the CCPA.

FAQ. 41 DOES THE CCPA'S STATUTORY DAMAGES APPLY TO SERVICE PROVIDERS?

The CCPA allows consumers whose personal information has been compromised in a data breach to recover hefty statutory damages of between $100 – $750 "per customer per incident or actual damages, whichever is greater."[126] The statutory damages provision provides incentives to plaintiffs' lawyers to pursue large class actions, even if the actions are based only on a single security incident.

But, the CCPA only imparts obligations directly upon a "business" – a term that is defined as a for-profit legal entity that collects personal information about California residents, "determines the purpose and means of the processing" of that information, does business in California, and hits one of the three threshold volume triggers set forth under the Act (*i.e.*, $25 million gross revenue, data about 50,000 Californians, or generates 50% of its revenue from selling personal information). If an entity is a "business" then all of the other obligations of the CCPA kick-in as well, such as the obligation to post a privacy notice, respond to consumer access requests, respond to consumer deletion requests, disclose the sale of consumer information, and offer consumers the ability to opt-out of such sales.

The statutory damages provision itself is tied to the definition of "business." It states: "[a]ny consumer whose nonencrypted or nonredacted personal information … is subject to unauthorized access and exfiltration, theft, or disclosure as a result of a *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 statutory damages.

In contrast, the CCPA defines a "service provider" as a for-profit legal entity that "processes information *on behalf of a business*, and is contractually prohibited from retaining, using, or disclosing that information for any purpose other than to provide service."[127] Unlike "businesses," the CCPA imposes <u>no</u> direct privacy obligations on service providers. Note, that the service provider would be subject to contractual retention, use, and disclosure restrictions. In addition, the service provider will likely be subject to a third-party claim brought by a business sued after a security breach by the service provider.[128]

The net result is that if a company falls under the definition of a "service provider," but does not fall under the definition of a "business," the CCPA imposes no statutory obligations upon it and does not subject it to statutory damages. That, of course, begs the question of whether a company might be both a "service

[126] CCPA, Section 1798,150(a)(1).

[127] CCPA, Section 1798.140(c).

[128] CCPA, Section 1798.140(v).

provider" and a "business." Theoretically, nothing within the CCPA precludes a dual designation, and, as the terms are currently defined, they do not appear to be mutually exclusive. To understand why, consider a hypothetical company (e.g., an accounting firm) that collects personal information on behalf of its client (e.g., while conducting an audit), has gross revenue of over $25 million, but is contractually bound not to use, share, or disclose that information other than to provide service. The company would satisfy the definition of a "service provider." The company would also satisfy every element of the definition of a "business" with the possible exception that it may not be intuitively clear whether the company "determines the purpose and means" of the processing.

In order to understand whether the hypothetical company could both be a "service provider" and determine the "purpose and means" of the processing, it is important to understand that the phrase "determines the purpose and means of the processing" was borrowed from the definition of a "controller" within the European GDPR.[129] In the context of the GDPR, European regulators examined whether a service provider that is generally bound to retention, use, and disclosure restrictions might also retain sufficient autonomy concerning the purpose and means of processing as to be classified under the GDPR as a "controller." The European regulators ultimately identified a non-exhaustive list of service providers that fit such a description including the following:

- Accountants;[130]
- Attorneys;[131]
- Mail delivery services (when providing tracking functionality);[132]
- Market research companies;[133]
- Payment processors;[134]and

[129] In comparison, the European GDPR imposes direct regulatory requirements on both "controllers" and "processors." Some of the obligations imposed by the GDPR apply equally to both groups, such as the obligation to take steps to secure data. Other obligations imposed by the GDPR apply only to one group or the other.

[130] Compare CCPA, Section 1798.140(C) to GDPR, Article 4(7).

[131] United Kingdom Information Commissioner's Office ("ICO"), *Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are* (2014) at 13.

[132] United Kingdom Information Commissioner's Office ("ICO), *Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are* (2014) at 12.

[133] United Kingdom Information Commissioner's Office ("ICO), *Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are* (2014) at 12.

[134] United Kingdom Information Commissioner's Office ("ICO), *Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are* (2014) at 10.

- Social network service providers that provide online communications platforms.[135]

There remains a great deal of uncertainty whether California courts will look to European regulators for guidance when interpreting the CCPA. Plaintiffs' attorneys are likely to argue that because European regulators have determined that various classes of service providers retain sufficient control over the purpose and means of processing to be considered "service providers" and "controllers," California courts should similarly find that such companies are "service providers" and "businesses" under the CCPA. If the argument succeeds, service providers may find themselves with the same regulatory obligations as their clients. From a litigation standpoint, both service providers and their clients may also become the targets of class actions aimed at recovering the large statutory damages authorized by the CCPA.

[135] United Kingdom Information Commissioner's Office ("ICO), *Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are* (2014) at 11.

FAQ. 42 DOES THE CCPA PERMIT NATIONWIDE CLASS ACTIONS OR ONLY STATE ACTIONS?

The CCPA applies only to information about a "consumer" – a term which is defined within the statute as including only "a natural person who is a California resident."[136] As a result, plaintiffs' lawyers pursuing class actions under the Act will be forced to narrow their actions to individuals residing in California, rather than out-of-state residents or legal entities affected by a data breach. Practically speaking, plaintiffs' lawyers will likely bring claims on behalf of non-California class members alleging various common law theories, although such theories may not be as successful as pursuing claims under the CCPA.

In comparison, the European GDPR is often misunderstood as only applying to data about European Union "citizens." In reality the scope of the GDPR varies based, in part, on which of two jurisdictional "hooks" apply to a company.

The first jurisdictional hook is found within Article 3(1) which purports to apply the GDPR to the processing of personal data in the context of activities of any "establishment" of a controller or processor in the European Union. If the GDPR is triggered because a company is established in the European Union an argument could be made that the GDPR is intended to apply to the processing of data relating to all data subjects – regardless of whether they are citizens or residents of the European Union, the United States, or of another country. Such an interpretation would align with the European Commission's statement that companies should respect the principles within the GDPR "whatever the[] nationality or residence" of a data subject.[137]

The second jurisdictional hook is found within Article 3(2) which purports to apply the GDPR to companies that are "not established in the Union" if they offer goods or services or monitor the behavior of "data subjects who are in the Union." The term "data subjects who are in the Union" refers to individuals that are physically present in the European Union regardless of their citizenship, nationality, or long-term residence. As a result, it theoretically could apply to United States citizens studying in Europe, vacationing in Europe, or temporarily travelling through Europe.

The CCPA's reach is, by definition, not as broad, providing some relief to companies facing a data breach with a national impact.

[136] CCPA, Section 1798.140(g).

[137] GDPR, Recital 2.

FAQ. 43 IS A SERVICE PROVIDER PERMITTED TO DISCLOSE PERSONAL INFORMATION IF IT RECEIVES A CIVIL SUBPOENA OR A DISCOVERY REQUEST?

Section 1798.140(v) of the CCPA states that a service provider must be contractually prohibited from "disclosing the personal information [provided to it by a business] 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*. . . ."[138]

Section 1798.145(a) of the CCPA contains six exceptions to the disclosure prohibitions. While one of those exceptions involves compliance with "a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities," the exception applies only to a "business."[139] As the Act defines "businesses" and "service providers" separately (the former determines the "purposes and means of the processing of consumers' personal information," the latter often does not) it appears that, on its face, the CCPA does *not* excuse some service providers from complying with its contractual obligation to not disclose information in order to comply with civil investigations, subpoenas, or summonses. This conclusion is bolstered by the fact that one of the other exceptions within Section 1798.145(a) (an exception that allows for disclosure when cooperating with law enforcement agencies) specifically references service providers.

While common sense suggests that a service provider should be able to comply with a lawfully issued subpoena or discovery request, given the text of the CCPA, it is unclear whether businesses can contractually permit their service providers to comply with civil discovery and, if they cannot, whether a service provider will be permitted to disclose information in response to discovery without being held in breach of contract.

Until the legislature or courts provide further guidance on this issue, service providers receiving civil subpoenas or discovery requests should consider asserting objections and/or seeking a protective order based on the CCPA, and withhold personal information from any production response until the parties can agree on excluding or redacting the personal information or a court orders production.

To avoid potential breach of contract issues, the parties may wish to provide within their contracts an instruction from the business to the service provider stating that (1) the service provider will forward any such requests to the business, and (2) the business will instruct the service provider on how to handle the request. Absent contrary judicial or legislative direction, the CCPA may even allow an instruction in

[138] CCPA, Section 1798.140(v).

[139] CCPA, Section 1798.145(a)(3).

the contract stating that the service provider is permitted to disclose the data in response to a validly submitted discovery request after providing the business with notice and an opportunity to object. Note that such an instruction under the CCPA may not be consistent with the GDPR, so there may be a slight contracting tension between a service provider that is required to comply with both laws.

FAQ. 44 DO ALL CYBER-INSURANCE POLICIES COVER LITIGATION UNDER THE CCPA?

Possibly. Most cyber policies cover both third party claims arising from a data security breach, including lawsuits brought by individuals whose data was exposed or compromised. The CCPA provides for the recovery of statutory damages of between $100-$750 per individual after a security breach in certain circumstances. Such claims would be covered under most cyber policies.

Whether a cyber policy would cover claims relating to data privacy violations (e.g., claims that a business misused personal data or did not provide individuals with rights of access under the CCPA) is an open question. Although the California legislature did not approve a private right of action for violations of the CCPA's privacy provisions, plaintiffs' counsel may still attempt to bring suits as violations of other laws, including consumer protection statutes. Some policies provide coverage for such claims, but some may not. You should carefully review the cyber coverage for both third party claims relating to data security breaches and privacy violations.

FAQ. 45 WHAT PROVISIONS WITHIN A CYBER-INSURANCE POLICY SHOULD BUSINESSES REVIEW WHEN DETERMINING WHETHER THEIR POLICY WILL COVER LITIGATION UNDER THE CCPA?

Litigation coverage would typically be found in the third party claim coverage of a cyber insurance policy. Most cyber policies will distinguish between a “security” event and a “privacy” event. A security event will generally involve the unauthorized access to or acquisition of personal information or personal data. A privacy event will generally relate to violations of privacy laws that set forth what companies can or cannot do with personal information and the rights afforded to individuals concerning data about them held by a company subject to those laws. In reviewing a policy, careful attention should be made to ensuring that the third party claim coverage includes coverage for litigation arising from both security events and privacy events.

FAQ. 46 WHAT FACTORS SHOULD A COMPANY CONSIDER WHEN EVALUATING AN ATTORNEY TO DEFEND A CCPA CLAIM?

Typically, a law firm defending a CCPA claim should have a strong background in both litigation and data privacy and security. For security breaches, the CCPA expressly contemplates that lawsuits brought by individuals affected by a breach may be brought as class actions. Accordingly, legal counsel familiar with the requirements for class certification and the class settlement process will best position the company to defend itself. However, because privacy and security issues have developed into a stand-alone, specialized area of the law, counsel with deep expertise in this subject matter will also serve the company well in court.

FAQ. 47 WHAT IS THE STATUTE OF LIMITATIONS FOR CLAIMS BROUGHT PURSUANT TO THE CCPA?

The CCPA itself does not contain a limitations period, but, like many states, California has within its rules of civil procedure omnibus limitations periods that apply to statutes for which a limitations period is not otherwise set. That source gives two possibilities depending upon the type of suit initiated:

- <u>Four Years</u>. Code of Civil Procedure section 343, is the "catch-all" statute of limitations, providing that "an action for relief not hereinbefore provided for must be commenced within <u>four years</u> after the cause of action shall have accrued." Net result it is possible that someone (e.g., the AG) could argue that the limitations period runs for four years. The net result is that if you were to do something like collect a consumer's consent to transmit information to a third party (in order to take it out of the definition of "sale") the best practice would be to keep the documentation of that consent for four years.

- <u>Three Years</u>. Pursuant to Code of Civil Procedure section 338, subdivision (a), the default statute of limitations that generally applies to actions for *personal injuries* based on *statutory violations*, is three years. Specifically it applies to "[a]n action upon a liability created by statute …."[140] The net result is that if a consumer is given a private right of action (or figures out a workaround to create a private right of action), their period for filing suit would likely be three years.

[140] Code Civ. Proc., § 338, subd. (a).

FAQ. 48 CAN COMPANIES USE ARBITRATION CLAUSES AND CLASS ACTION WAIVER PROVISIONS TO MITIGATE THE RISK OF CCPA-RELATED CLASS ACTIONS?

More than likely.

The CCPA states that consumers may seek, on "an individual or class-wide" basis, actual damages, statutory damages, or injunctive or declaratory relief following certain types of data security breaches.[141] The CCPA further states that "[a]ny provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under [the CCPA], including, but not limited to, any right to a remedy or means of enforcement" is "void and unenforceable."[142] The reference to contract provisions limiting consumer rights as being void and unenforceable has led some plaintiffs' attorneys to suggest that the California legislature intended to invalidate the use of arbitration and class action waiver clauses in contracts as those provisions might prevent consumers from proceeding on a "class-wide" basis.

Despite the language in the CCPA, the United States Supreme Court has consistently affirmed the strong federal policy favoring arbitration and the enforceability of class action waivers in arbitration agreements. In the landmark case of *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2011), the Supreme Court explained that the Federal Arbitration Act ("FAA") was specifically designed to pre-empt state laws that undermine the goal of the FAA to promote arbitration. Furthermore in *Sanchez v. Valencia Holding Co.,* 61 Cal. 4th 889 (2015), the California Supreme Court determined that class action waiver provisions within contracts are enforceable even if a state law appears to provide for class action type recovery.

As a result, and based upon the holdings in *Concepcion* and *Sanchez*, there is a strong argument that the CCPA will not be interpreted as preventing consumers from entering into arbitration agreements or from agreeing to waive their ability to proceed in class actions.

[141] Cal. Civ. Code § 1798.150.

[142] Cal. Civ. Code. § 1798.192.

FAQ. 49 CAN COMPANIES ASSERT AS A DEFENSE TO CCPA LITIGATION THAT THE STATUTE VIOLATES THE DORMANT COMMERCE CLAUSE?

Quite Possibly.

The Commerce Clause[143] of the US Constitution gives the US Congress the power to regulate commerce between the states. While states may generally regulate wholly *intra*-state commerce, when they attempt to regulate *inter*-state commerce they may run afoul of the Dormant Commerce Clause. The Dormant Commerce Clause is a function of law that acts to protect the negative implications of the Commerce Clause by generally prohibiting state legislatures from unduly burdening out-of-state commerce, discriminating against out-of-state commerce, or regulating commercial conduct that occurs wholly outside of their state.

The Drafters of the CCPA, therefore, took care to attempt to draft the CCPA in a way that would avoid Dormant Commerce Clause challenges -- the law does not facially discriminate against out-of-state actors since it applies equally to companies located both within and outside the State, and it also does not seem to have an impermissibly protectionist purpose or effect. The primary two issues with the CCPA that could likely be asserted with a Dormant Commerce Clause defense, therefore, are (i) that the CCPA's adverse effect on interstate commerce is disproportionate to legitimate California interests in protecting the privacy of California residents, and (ii) that the CCPA regulates wholly out-of-state commercial conduct.

The expansive definitions and broad scope of the CCPA and the changes that out-of-state companies have to make to their data collection practices for all data, not simply data pertaining to California residents, will almost certainly lead to litigation in this area and time will tell how the courts will respond. Courts will have to balance California's interests in protecting their residents' privacy against the burden imposed on out-of-state companies to determine if it is disproportionate. Furthermore, the broad definitions in the CCPA purport to allow it to apply to out-of-state companies with little or no connection to California, such as service providers or third parties whose only business with California is receiving personal information about a California resident from another entity. Whether or not the courts find this to be a sufficient relationship to California to constitute intra-state commerce remains to be seen. Overall,

[143] US Constitution, Article 1, Section 8, Clause 3

however, there is the possibility of asserting the Dormant Commerce Clause as a defense to CCPA litigation, although the outcome remains unclear.

FAQ. 50 CAN COMPANIES ASSERT AS A DEFENSE TO CCPA LITIGATION THAT IT IS VOID FOR VAGUENESS?

Quite Possibly.

The doctrine of "Void-for-Vagueness" holds that a law is void if it is written in such a way as to prevent an ordinary person from being able to understand what is forbidden and what is permissible under the law so as to permit arbitrary enforcement.[144] A law may also be invalidated under the doctrine if it is overly broad.

The CCPA suffers from definitions and restrictions that seem to be both insufficiently defined and overly broad, leaving the Act ripe for a vagueness challenge. It would not be too far a stretch to argue that an ordinary person would not know what was prohibited or permitted when deciding whether to disclose loyalty program valuations, for instance. Likewise, the fact that the definition of "personal information" under the CCPA includes any information that is "reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer of household"[145] can leave a business without adequate guidance to determine whether a given piece of information is personal information under the CCPA. When one considers the myriad consequences that may result from a misunderstanding and misapplication of the CCPA's provisions, a void-for-vagueness argument could possibly be made on these grounds.

Several of the definitions contained within the CCPA could also be argued to be overly broad. The "personal information"[146] definition discussed above could theoretically encompass almost all data. The definition of "business"[147] and "sale"[148] could also theoretically cover many out-of-state businesses that have little or no other contact with California, running into Dormant Commerce Clause concerns. For these reasons, there is a possibility of asserting a void-for-vagueness defense to CCPA litigation, although time will tell how the courts interpret the doctrine in relationship to the CCPA.

[144] *City of Chicago v. Morales*, 527 U.S. 41 (1999)
[145] CCPA, Section 1798.140(o)(1)
[146] CCPA, Section 1798.140(o)(1).
[147] CCPA, Section 1798.140(c)(1).
[148] CCPA, Section 1798.140(t)(1).

Text of the CCPA

TEXT OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018

(Last updated January 2020)

Table of Contents[149]

[149] 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, 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, fulfil the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' 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 that consumer’s 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 business' 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 – Information required to be provided as part of an access request

(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 consumer 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 consumers.

(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) That a consumer has the right to request 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 category of third parties 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 at least 13 years of age and less than 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 wilfully 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 business 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 business by the consumer's data.

(2) A business that offers any financial incentives pursuant to this subdivision shall notify consumers of the financial incentives pursuant to Section 1798.130.

(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 1798.130 that 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)

(A) 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. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

(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' 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' 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 may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer maintains an account with the business, the business may require the consumer to submit the request through that account.

(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 website and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 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' privacy practices or the business' compliance with this title are informed of all requirements in Sections 1798.100, 1798.105, 1798.110, 1798.115, and 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' 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 de-identified.

(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 that 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's 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's 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 that the personal information 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 behavior.

(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 non-commercial 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 website 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 1798.135, 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 reasonably 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 reasonably 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 website, 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. Sec. 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, behavior, attitudes, intelligence, abilities, and aptitudes.

(2) “Personal information” does not include publicly available information. For purposes of this paragraph, “publicly available” means information that is lawfully made available from federal, state, or local government records. “Publicly available” does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(3) “Personal information” 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 that 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 of 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.

(ii) 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.

(B) 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 1798.100, 1798.105, 1798.110, and 1798.115 if the business cannot verify, pursuant to 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' 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)

(1) This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of

information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, section 1681 et seq., Title 15 of the United States Code and the information is not used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act.

(3) This subdivision shall not apply to Section 1798.150.

(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)

(1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle’s manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) For purposes of this subdivision:

(A) “Vehicle information” means the vehicle information number, make, model, year, and odometer reading.

(B) “Ownership information” means the name or names of the registered owner or owners and the contact information for the owner or owners.

(h)

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

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person’s personal information is collected and used by the business solely within the context of the natural person’s role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(E) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (b) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2021.

(i) Notwithstanding a business' 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.

(j) 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.

(k) This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(l) 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.

(m) 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 non-commercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

(n)

(1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, non-profit, or government agency.

(2) For purposes of this subdivision:

(A) “Contractor” means a natural person who provides any service to a business pursuant to a written contract.

(B) “Director” means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) “Officer” means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) “Owner” means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2021.

1798.150- Civil actions

(a)

(1) Any consumer whose nonencrypted and 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 wilfulness 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 -Pre-emption

This title is a matter of statewide concern and supersedes and pre-empts 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 Section 1798.120.

(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's determination that a request for information received from 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 follows:

(1) To establish rules and procedures on how to process and comply with verifiable consumer requests for specific pieces of personal information relating to a household in order to address obstacles to implementation and privacy concerns.

(2) 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's 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

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

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

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

Jennifer Jackson
Partner
Litigation and Corporate Risk
T: +1 310-576-2360
jjackson@bclplaw.com

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

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

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

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

Merrit Jones
Counsel
Commercial Disputes
T: +1 415-675-3435
Merrit.Jones@bclplaw.com

Sara Markert
Counsel
Commercial Disputes
T: +1 949-301-6729
Sara.Markert@bclplaw.com

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

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

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

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

Andrea Maciejewski
Associate
Boulder, Colorado
T: +1 303-417-8514
Andrea.Maciejewski@bclplaw.com

Goli Mahdavi
Associate
San Francisco, California
T: +1 415-675-3448
Goli.Mahdavi@bclplaw.com

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

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

Anne Redcross Beehler
Associate
Irvine, California
T: +1 949-223-7185
AnneRedcross.Beehler@bclplaw.com

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

Sarah Schenker
Associate
Chicago, Illinois
T: +1 312-602-5097
Sarah.Schenker @bclplaw.com

Sheek Shah
Associate
Chicago, Illinois
T: +1 312-602-5103
Sheek.Shah@bclplaw.com

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

www.bclplaw.com