Tricky Topics in CCPA Compliance

By Marc J. Zwillinger, Kandi Parsons, and Michelle Anderson[1]

This article was originally published in the Media Law Resource Center Bulletin, "Legal Frontiers in Digital Media" (Spring 2019)

At the time of the writing of this article, the final language of the California Consumer Privacy Act ("CCPA") is yet to be determined. Nevertheless, given the effective date of the statute, as well as the requirement to provide California consumers with access to their personal information ("Personal Information" as defined by the CCPA) for the 12-month period preceding a consumer's request, many companies have begun CCPA preparations in earnest. Providing definitive guidance on CCPA compliance absent the final statutory language and prior to guidance from the Attorney General's ("AG") office, however, is challenging. In addition to the many drafting errors spotted by privacy commentators, several sections of the CCPA are susceptible to conflicting interpretations—often as a result of statutory language that appears at odds with the statute's stated purpose. To date, most commentators have focused on supporting specific big-picture curative amendments, while subtler aspects of the statute have received less attention and are unlikely to be materially altered by the currently pending amendments.

This article addresses some of the more complicated parts of CCPA compliance by responding to the types of practical questions we have been asked. One additional purpose of this article is to build industry consensus for the interpretations set forth below and to highlight additional issues that could use further clarification through either legislative amendment or AG guidance. These topics include: (1) which specific pages must contain the "Do Not Sell My Data" links; (2) what types of verification procedures are appropriate for access and deletion requests, especially when such requests are submitted on behalf of consumers by someone else; (3) how consumers can be encouraged to create accounts to request or receive their data; (4) whether disclosures to a service provider where the service provider still retains the right to use some of the data for its own operational purpose make the service provider a third party, potentially subject to the CCPA's requirements regarding the sale of Personal Information; (5) whether the CCPA requires businesses to locate Personal Information contained in unstructured data, such as in surveillance footage or email text; and (6) what aspects of a media organization's functions are outside the scope of the CCPA.

1. Is a "Do Not Sell My Personal Information" Link Required on Every Webpage?

The CCPA requires businesses that "sell" Personal Information to place a clear and conspicuous link that says, "Do Not Sell My Personal Information" (i) on the business's homepage; (ii) in its online privacy policy(ies); and (iii) in any California-specific description of consumers' privacy rights.[2] At least one aspect of this obligation seems clear: entities that sell Personal Information

[1] Marc Zwillinger, Kandi Parsons, and Michelle Anderson are attorneys at ZwillGen PLLC. All three attorneys counsel clients on a wide variety of privacy and information security issues, including CCPA compliance. All views expressed in this article are the authors' personal observations, and should not be attributed to ZwillGen, any of its other attorneys, or any of its clients.

[2] California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, at § 1798.135(a) (2019) [hereinafter CCPA], *available at* http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121. Alternatively, the CCPA doesn't require a business to post a "Do Not Sell My Personal Information" link on its public homepage if it maintains a separate and additional homepage dedicated to California consumers, includes the required text and

must include a "Do Not Sell My Personal Information" link in their online privacy policy(ies), such as those required under the California Online Privacy Protection Act ("CalOPPA") and the CCPA itself.[3]

Complying with a requirement to place a link on a homepage would seem to be straightforward. But the CCPA's definition of "homepage" not only fails to align with a common sense understanding of the term, but also undermines any narrowing intended by including a location element as part of the link requirement. Although a homepage is typically considered to be the introductory page of a website, under the CCPA, a "homepage" is both the introductory page *and* "any Internet Web page where Personal Information is collected."[4] Because the CCPA's expansive definition of Personal Information includes information such as IP address, which is collected on every webpage in order for a website to function, a strict reading of the statute would lead to the conclusion that any page is a "homepage." If the CCPA intended for the link to be posted on every webpage, drafters could have easily and unambiguously required posting on every page. But the CCPA specifically does not do so. In fact, for mobile applications it specifies that "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 [required] notice."[5] These nuanced definitions clearly suggest that not every screen a consumer sees is required to have the link and that only a subset of pages is clearly contemplated by the law.

A better reading of the CCPA is that it requires a link on (i) a website's initial landing page; (ii) any page where a consumer would reasonably look to read about the business' privacy and consumer rights policies; and (iii) on all webpages where consumers directly input information, such as webpages that enable consumers to fill in an account profile or register, provide an email address to request more information, or complete other open forms or fields. Placing the link on all initial and information pages and where consumers ***actively*** provide their Personal Information is consistent with the statute's goal of enabling consumers to opt out of the sale of information they input and gives actual meaning to the definition of homepage.[6] Of course, businesses who sell Personal Information may find it easier to operationalize placing the link on

---

links on that California-specific homepage, and takes reasonable steps to ensure that California consumers are directed to that California-specific homepage. CCPA at § 1798.135(b). However, creating and maintaining a California-specific homepage, and taking "reasonable steps" to appropriately route all California Internet, may present a significant administrative burden that makes this compliance path less appealing.

[3] Cal. Bus. & Prof. Code §§ 22575-79 (2019), *available at* https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC.

[4] CCPA, *supra* note 2, at § 1798.140(l).

[5] *Id.*

[6] This reading is consistent with the AG's CalOPPA guidance, which says privacy policies should be linked to on "every web page where personal information is collected." Attorney General Kamala Harris, *Making Your Privacy Practices Public* (May 2014), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf. Notably, under CalOPPA the definition of personal information did not include the types of information that every webpage automatically collects.

every page, but those that can implement a more tailored approach may prefer to limit the placement of the link.

A more aggressive approach would be to limit the do-not-sell link to those pages where consumers input information that will be sold. Although this would align with the general principle of providing just-in-time notice most relevant to the data that is being collected, the statute does not support this more narrowly targeted approach. Rather, the statute suggests that the notice has to be in all places where a consumer would reasonably look to learn about the organizations' privacy practices.[7] Just as drafters could have indicated the link must be on every webpage, they could have easily limited its placement to those webpages where the collection of information that is sold occurs.

For online services like mobile applications, the CCPA requires that businesses provide a do-not-sell link at (i) the places the online service can be accessed or downloaded, such as a log-in page or in the app store enabling consumers to see the link before downloading the service; and (ii) within the service, such as in a settings and About section of the service, so users can exercise their opt-out right either before downloading the application or after accessing or downloading the service.[8] Notably, the language does not give businesses the option to choose one of these locations, but indicates that each of these is a homepage, thus requiring the do-not-sell link.

2. How Should I Verify Consumer Requests?

Absent certain exceptions, businesses must honor consumers' requests for access and deletion in response to "verifiable consumer requests." The CCPA specifically states that a business may only honor requests for access that it can verify.[9] A consumer may make a verifiable consumer request on his/her own behalf or on behalf of the consumer's minor child, and a natural person or person registered with the Secretary of State may also make a request on behalf of the consumer, provided they are authorized to act on the consumer's behalf. The statute defines a "verifiable consumer request" as a request by a consumer that a business can "reasonably verify, pursuant to regulations adopted by the Attorney General."[10] The AG has until July 1, 2020, to issue such regulations, though the CCPA mandates that the regulations consider a request submitted through a password-protected account maintained by a consumer with the business while the consumer is logged into the account to be a verifiable consumer request.[11]

---

[7] Similarly, the plain language of the CCPA also requires that a "Do Not Sell My Personal Information" link be included in any descriptions (whether online or not) about California consumers' rights (though whether the legislature intended for this disclosure to be required for both online and offline disclosures is uncertain).

[8] CCPA, *supra* note 2, at § 1798.140(l).

[9] *Id.* at § 1798.140(y). Notably, the statute does not specifically prohibit businesses from deleting information where the request cannot be verified. We certainly believe, however, that businesses should not delete information based on third-party requests if they cannot verify that the third-party is authorized to act on the consumers' behalf.

[10] *Id.*

[11] *Id.* at § 1798.185.

For now, in the absence of AG guidance, we recommend that businesses develop a verification matrix that sets out particular methods of establishing a link between the requestor and the consumer whose data is at issue that are proportional to the risk posed by consumer's request.[12] The risks vary depending on the nature of the request (access is riskier than deletion), the sensitivity or invasiveness of the information at issue (with data like geolocation information or medical information constituting higher risk than requesting access to a name and contact information), and the identity of the person making the request (because requests by a third party on behalf of a consumer present a higher risk).

a. Verifying Requests from Consumers on Their Own Behalf

For requests made by consumers on their own behalf, we recommend that, when possible, businesses verify the consumer's identity using information the consumer has already provided. For example, if a consumer calls to request information about his/her account, the business could require the consumer to submit the request using the email address the consumer uses with the business. Where a consumer requests more sensitive Personal Information, businesses should ask for additional information in a manner that is consistent with the principles of necessity and proportionality. For example, businesses should not collect new forms of sensitive Personal Information in order to respond to a request for video viewing history. Instead, to verify consumers making a request for their video viewing history, the business could require consumers to answer knowledge-based questions about past video-viewing, purchase transactions, or linked accounts.

Businesses should always keep in mind, however, that all verification requests provide an attack vector for obtaining Personal Information about consumers. Similar to how early attempts at "forgot my password flows" provided mechanisms for hackers to access accounts, a business could create liability—in forms that include a private right of action—by allowing unreasonably easy methods of verification, as the statute provides no safe harbor. In terms of practical risk, more rigorous verification standards (or over verifying) create less risk than less rigorous verification standards (under verifying). Accordingly, for very sensitive information, businesses can use time-honored verification methods, such as in-person ID inspection, third-party online verification services, or traditional paper-based verification, such as affidavits, that provide forms of recourse and barriers to third-party identify fraud attempts.

b. Verifying Requests from Individuals on Behalf of a Consumer

When an individual makes a request on behalf of someone else, businesses should also ask for information necessary to verify both the identity of the requestor *and* the requestor's authorization to make the request. The level of verification businesses require for access requests should be proportional to the enhanced risk that providing information to the requestor could result in inadvertently giving information to a stranger or a party adverse to the consumer,

[12] This is consistent with guidance from guidance from EU regulators and advisors. *See e.g.*, Article 29 Working Party, *Guidelines on the right to "data portability"* (WP242 rev.01), 14 (Apr. 5, 2017), *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233; Information Commissioner's Office, *Subject Access Code of Practice*, 23-25 (June 9, 2017), *available at* https://ico.org.uk/media/2259722/subject-access-code-of-practice.pdf.

such as an opposing party in a lawsuit—or worse, someone dangerous to the consumer, such as a stalker.

For example, if someone requests access to Personal Information on behalf of an incapacitated parent, the consumer should (i) request proof of the authorization from the consumer to appoint the requestor (such as a letter from an attorney or Power of Attorney appointing the requestor, which the business can try to independently verify with the attorney or through the account to confirm the appointment); (ii) request information to verify the requestor's identity (such as a copy of a driver's license to match the name on the Power of Attorney or a copy of a birth certificate showing the consumer as his/her parent); and (iii) if the request is by an entity, verify the entity's registration record with the California Secretary of State to ensure that there is recourse.

While these steps may insert some obstacles into what is intended to be an accessible process, the risks of responding to an unverified third party's request—particularly a request for access—are too great to require less. This is especially true in light of the fact that providing certain types of a consumer's Personal Information to an unauthorized third party under California's breach notification law would qualify as a security breach.[13] Steps taken to verify a third-party requestor are thus not only to satisfy CCPA requirements but also to avoid providing unsecured Personal Information to unauthorized third parties.

c. Deletion Requests

In considering how to verify a deletion request, businesses should consider imposing less rigorous standards than for access requests. Generally, a business's obligation to provide *access* to Personal Information can present the risk of fraud or safety to their customers and attendant liability for the company. In contrast, the risks generally associated with the deletion of data in response to a fraudulent request are less significant. Deleting sensitive data, for example, will not likely facilitate identity theft, phishing, or stalking. As such, most businesses can reasonably accept deletion requests that come from or are confirmed via a response from the email on file for that consumer. In certain limited circumstances, the type of Personal Information held or business considerations may warrant implementing more stringent verification requirements. For example, businesses that are custodians of data, such as cloud storage providers, may impose higher standards before deleting such data. Businesses that receive deletion requests that could be in an effort to destroy evidence related to a possible crime, like precise geolocation data held by a rideshare providers, also may implement a different and slower process. Considering the risks that would be associated with errant deletion of its data will help a business determine what to require to verify such requests in its verification matrix.[14]

---

[13] Cal. Civ. Code § 1798.82(g) (2019), *available at* http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82.

[14] We note also that there are a number of exceptions to the right to deletion that don't exist for the right to access, such as exceptions to deleting Personal Information to complete a transaction, detect security incidents, or exercise free speech. Such exceptions mean a business may be able to deny a right to delete even before verifying the requestor.

3. Can Consumers Be Required or Encouraged to Create an Account to Exercise Certain Rights or to Receive Information Electronically?

Although the CCPA allows consumers to make verifiable consumer requests for access through their online accounts with a business, the CCPA prohibits businesses from *requiring* that consumers create accounts in order to exercise their rights. The CCPA dictates that businesses cannot require consumers to create an account to direct businesses to stop selling their Personal Information.[15] In other words, businesses cannot force account creation on consumers seeking to exercise their right to opt-out. Nor can businesses require that consumers create an account "in order to make a verifiable consumer request" for access or deletion.[16] This prohibition eliminates one common way that businesses verify their customers and creates tension with the demand that businesses respond to *verifiable* consumer requests. Indeed, the *only* example of a verifiable consumer request included in the CCPA is that requests made by consumers while logged into their password-protected accounts are considered verifiable consumer requests.[17]

But even if account creation is prohibited for making a consumer request, the CCPA does not strictly prohibit mandatory account creation for electronic delivery of the requested information. Under the CCPA, businesses are required to make disclosures "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 the information from one entity to another entity without hindrance."[18] Some businesses have noted that the account creation for delivery is not strictly prohibited and are considering requiring account creation for delivery. However, a consumer would not be able to exercise a meaningful option to receive the information by mail or electronically in every case if account creation was a prerequisite to electronic delivery. Thus, to give meaning to the "consumer's option" language, we do not believe account creation—even for delivery of information—can be required.

However, the CCPA does not prohibit businesses from *encouraging* consumers to create accounts, such as by offering incentives for account creation. For example, a business could offer to respond to verifiable consumer requests faster (e.g., within 10 days instead of 45 days) that are made through an account. Similarly, a business could provide consumers who create accounts with easier mechanisms for tailoring requests through an account, such as with drop-down menus that allow a consumer to request particular types of information from a particular division of a business.

Privacy advocates may argue that such incentives violate the CCPA's anti-discrimination rules. Under the CCPA, businesses may not discriminate against a consumer because the consumer exercised his/her CCPA rights, including by "providing a different level or quality of goods or services to the consumer."[19] However, incentivizing account creation would not constitute

---

[15] CCPA, *supra* note 2, at § 1798.135(a)(1).

[16] *Id.* at § 1798.130(a)(2).

[17] *Id.* at § 1798.140(y).

[18] *Id.*

[19] *Id.* at § 1798.125(a)(1)(C).

discrimination, as there is no "right" that is being exercised in this context. Rather, consumers have rights to access, delete, or opt-out of the sale of their Personal Information—not a "right" to not have to create an account. Incentivizing account creation would create different levels of service in responding to requests based on the method by which the request was made, not based on the fact that the consumer exercised a right.

Moreover, even if the anti-discrimination provisions applied to account creation, the CCPA permits businesses to offer incentives to consumers for the collection, sale, or deletion of Personal Information as long as the incentive "is directly related to the value provided to the consumer by the consumer's data."[20] Setting aside the open question of exactly what is meant by "the value provided to the consumer by the consumer's data," we believe that if a consumer derives value from an account creation incentive, then such an incentive is not only permitted but contemplated by the CCPA.

4. Does a Disclosure to a Service Provider that Retains the Right to Use Personal Information for Its Own Operational Purpose Makes the Service Provider a Third Party?

In order to qualify as a service provider under the CCPA, an entity must process information on behalf of a business for **a business purpose** pursuant to a written contract that prohibits the service provider from retaining, using, or disclosing 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 the CCPA, "including [prohibiting the service provider from] retaining, using, or disclosing the [Personal Information] for a commercial purpose other than providing the services specified in the contract with the business."[21] If an entity is a service provider, then it is not subject to the CCPA compliance obligations relating to businesses and third parties, such as honoring requests to opt out of the sale of Personal Information to a third party.[22]

Some have argued that if a service provider uses Personal Information for its own purposes then it no longer can be a service provider because it is not handling the Personal Information solely on behalf of the business. But we do not read the definition this narrowly. We believe that if an entity satisfies all of the service provider requirements (and all of the requirements to not be a third party)—and the entity uses Personal Information for its own operational purposes—it is still a service provider. First, by definition, a service provider must be prohibited from using

[20] *Id.* at § 1798.125(b)(1).

[21] *Id.* at § 1798.140(v).

[22] A business is an entity that "alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information" and meets certain thresholds. *Id.* at § 1798.140(c). A third party is any entity that is neither a business nor a person to whom a business discloses a consumer's Personal Information for a business purpose pursuant to a written contract, provided that the contract prohibits the third party 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; or (iii) retaining, using, or disclosing the information outside of the direct business relationship between the third party and the business. *Id.* at § 1798.140(w).

Personal Information *except* "as otherwise permitted" by the CCPA. Nothing in the CCPA prohibits a service provider from using Personal Information for its own operational purposes. Thus, assuming that a business' contract doesn't enforce greater limitations on a service provider, the service provider should have discretion to use Personal Information as permitted by the CCPA.

In addition, the term "business purpose" is defined to include both a business' *and* a service provider's operational purposes and the definition of service provider allows disclosure of Personal Information for a business purpose, without limitation as to whose business purpose is being satisfied.[23] This suggests that operational purposes, such as auditing and detecting security incidents, as well as those required to provide the provider's services, such as maintaining accounts or providing customer service, are valid purposes for both businesses and service providers and do not disqualify an entity from being a service provider.

5. Must a Business Locate Personal Information in Unstructured Data in Response to Access and Deletion Requests?

Suppose a large California gas station chain has surveillance cameras at all of its locations, and a California consumer who uses the gas station asks for copies of all video footage taken outside of any branch—unrelated to a particular transaction—where her face is captured. The consumer supplies a photograph of her face and verifies her identity. Must the gas station comply? Even though the consumer's face is considered Personal Information under the statute, we think the gas station need not search their videos for such footage.

The CCPA 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."[24] However, the CCPA *does not require* companies to "reidentify or otherwise link information that is not maintained in a manner that would be considered personal information" in order to respond to a consumer request.[25] In addressing the disclosure of consumer data, the law repeats this limitation: "This section does not require a business to do the following…otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information."[26]

The scope of a businesses' obligation under the CCPA therefore turns on what the California legislature meant by "**information that is not maintained in a manner that would be considered personal information.**" This language must be referring to information that is different from information that is deidentified or that is not Personal Information—as deidentified or non-personal data is outside the scope of the CCPA. It also appears to turn on how the business maintains or stores the information, in part, because the manner of storage is closely related to how easily the information can be located and retrieved. We believe that the

[23] *Id.* at § 1798.140(d).

[24] *Id.* at § 1798.140(o).

[25] *Id.* at § 1798.145(i).

[26] *Id.* at § 1798.110(d)(2).

logical interpretation of the phrase "not maintained in a manner that would be considered personal information" is that if a business does not, in the ordinary course, store information in such a way that it is part of a consumer profile or that can be reasonably associated with a particular individual or household, the business does not have to link the data to the consumer in response to a consumer's access or deletion request.[27]

Thus, for many businesses, including the California gas station chain in question, masses of undifferentiated or unstructured data (e.g., images contained in a video, faces in photographs, or text in the body of emails), as opposed to structured data (e.g., email header data, account data), would not likely be maintained in a manner that is Personal Information for which a business would have to respond to a request to exercise CCPA rights. This is likely true even if, for example, undifferentiated video footage contains a person's face (which would otherwise be Personal Information), or an email contains a person's name (which is undoubtedly Personal Information). This conclusion would likely not be true, however, if the data was created for the purpose of identifying and isolating individual data within the crowd footage.[28]

An alternative conclusion would upend the California AG's long-standing advocacy of the principle of "data minimization" because it would force businesses to make connections between data elements that are not reasonably needed for the purposes for which the data was collected.[29] Indeed, it would likely require businesses to combine and identify more data or utilize identifying technologies (e.g., facial recognition) than before, potentially creating highly detailed consumer dossiers that would not have otherwise existed.[30] In addition, it would also be inconsistent with the purpose of the statute to limit the power of businesses to amass data about consumers and combine and use it in ways that do not benefit consumers, such as by selling it.

This interpretation is further supported by the fact that the CCPA does not require businesses to respond to consumer requests that are "excessive."[31] When a request is "excessive" under the CCPA is not well defined, and the burden of showing excessiveness falls on the business. If the law were interpreted to require linking of all unstructured data, then it would force businesses to engage in excessive discovery-like searches and production processes in order to respond to

---

[27] This interpretation is consistent with a proposed amendment to the definition of Personal Information, which would revise the current exception to CCPA compliance for data that is not maintained in "a manner that would be considered personal information" to "data that is not maintained as personal information." California Consumer Privacy Act of 2018, AB 873 (2019-2020 Leg. Sess.) (2019), *available at* http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB873.

[28] For this example, if a person's face is captured and stored during every transaction through an ATM at a bank and linked to the person's bank profile and transactional record, the bank may have to comply with a CCPA access request.

[29] *See e.g.*, Kamala D. Harris, Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem*, at 9 (Jan. 2013), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf?.

[30] *See* Californians for Consumer Privacy, *About Us*, https://www.caprivacy.org/about-us (last accessed Mar. 25, 2019) (saying, e.g., "Your life is not their business.").

[31] CCPA, *supra* note 2, at § 1798.145(g)(3).

nearly every access request, even though the business itself was not using the data as Personal Information for its own purposes.

Absent contrary guidance, and in light of the statute's 30-day cure period, businesses have firm ground to push back on requests for unstructured data. They can argue (i) that businesses are not required to link such data where it is not maintained as Personal Information and (ii) even if unstructured data were deemed to be the type of Personal Information that must be provided or deleted, then businesses don't have to honor such access or deletion requests because doing so would be excessive.

6. What Aspects of a Media Organization's Operations Are Outside the Scope of the CCPA?

The first version of the CCPA accounted for the freedom of the press by carving out from commercial purposes the act of "engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism."[32] But legislators thought it would not go far enough in protecting the constitutionally granted rights of journalists. In September 2018, the California legislature amended the CCPA to exempt businesses from compliance with the CCPA requirements to the extent that such requirements "infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution."[33]

Section 2 of Article I of the California Constitution generally applies to freedom of the press. Subdivision (b) protects publishers, editors, reporters, and other persons connected with or employed by a newspaper or other related news organizations, including radio and TV stations, from having to make certain disclosures. In particular, the relevant Constitutional provisions indicate that such persons may not be found to be in contempt for refusing to disclose the **source of any information** or refusing to disclose any **unpublished information** gathered, received, or processed for communication to the public, such as notes, outtakes, photographs, tapes, or other data.[34]

In light of the California legislature's clear intent to exempt news organizations from complying with CCPA requirements relating to journalistic activities, we believe that such organizations need not comply with the CCPA's access and deletion requirements for activities such cultivating sources, conducting interviews and investigations, taking notes, taking photographs or making audio or video recordings, collaborating with other members of the press, protecting the identity of reporters in undercover investigations, preparing materials for publication, and publishing news or opinions for public consumption. Technically, the freedom of the press exception applies only "to the extent" that compliance with the CCPA would interfere with journalists' noncommercial activities. As such, some CCPA requirements, such as transparency

---

[32] *Id.* at § 1798.140(f). *Compare with* AB 375 (2017-2018 Leg. Sess.) (2018), *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[33] *Id.* at 1798.145(k).

[34] California Constitution, Art. 1 § 2, *available at* https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CONS&division=&title=&part=&chapter=&article=I.

or providing general information in response to access requests (e.g., the types of information collected from sources), arguably would still apply because they are unlikely to interfere with those journalistic activities. That said, we do not think that this is likely to be an enforcement priority.

News organizations *do*, however, need to comply with the CCPA for commercial activities, which include all activities required to operate the media organization as a money-making business. They include obviously commercial activities, like placing ads in hard-copy publications, serving digital ads, sending marketing emails, and creating and fulfilling subscriptions. In addition, the CCPA would apply to parts of larger media companies that are not related to journalism. For example, if a media organization owned a book publishing company or an advertising company, those publishing and advertising companies would still be subject to the CCPA.

7. Conclusion

With the final legislative text up in the air, and without AG guidance, some of the "tricky" aspects of CCPA guidance described in this article may eventually be superseded or confirmed by events. In all likelihood, many of the questions we have posed will remain unanswered even when the law goes into effect. As such, businesses may find this article useful in providing interim perspective as they begin their compliance efforts and further discussion of these topics may prompt the AG's office to recognize where additional regulatory guidance may be helpful.