NAI Analysis of Verifiable Consumer Requests Under the CCPA

V1.0

September 2019

About the NAI

Founded in 2000, the Network Advertising Initiative (NAI) is the leading self-regulatory organization representing third-party digital advertising companies. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing high standards for data collection and use for digital advertising in multiple media, including web, mobile, and TV.

Acknowledgments

This document was prepared by participants in the NAI's CCPA Implementation Working Group, a joint effort consisting of leading CCPA experts from NAI member companies and the NAI staff. Quantcast and MediaMath in particular made major contributions to developing this analysis.

Contact

Tony Ficarrotta (tony@networkadvertising.org)
Counsel, Compliance & Policy, NAI

Table of Contents

I. Introduction

A. Background on the CCPA

The California Consumer Privacy Act (CCPA)[1] is the first comprehensive consumer privacy law in the United States, and is expected to apply to virtually all ad-tech companies, publishers and advertisers that do business in California. This is because the law reaches all California "businesses" — a term defined to include, among other things, any for-profit business entity that sends or receives for a commercial purpose the personal information (PI) of 50,000 or more California consumers, households, or devices when that business entity determines the purposes and means of the processing of such information.[2] Further, as "personal information" is defined broadly to include cookie IDs, IP addresses, probabilistic identifiers, etc., many ad-tech use cases that rely on user-level information likely involve covered PI.[3]

So, while there are several complex defined terms to parse within the definition of "business," ad-tech companies that have reason to believe they process 50,000 or more IP addresses, cookie IDs, or mobile ad IDs connected to California consumers[4] or devices per year likely are covered "businesses," although they may also be "service providers"[5] or "third parties"[6] with respect to some of their business activities or in relation to some of their business partners.

The CCPA is often compared to the EU's General Data Protection Regulation (GDPR),[7] and while there are many substantive differences between the two frameworks, there are also important areas of overlap. In particular, the CCPA gives consumers: (1) the right to request that a business provide to them the "categories and specific pieces of personal information" the business has collected about them (and certain related information, such as the categories of sources of such PI, and the categories of third parties the businesses may share the information with),[8] which is comparable to the "right of access"

---

[1] CAL. CIV. CODE §§ 1798.100 *et seq.*

[2] *See id.* § 1798.140(c).

[3] Under the CCPA, "personal information" is 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[.]" It explicitly includes IP address, internet or other electronic network activity, device identifiers, cookies, beacons, pixel tags, mobile ad identifiers, probabilistic identifiers, and many other kinds of information frequently used in programmatic advertising, if such information identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household. *Id.* § 1798.140(o)(1).

[4] The CCPA defines "consumer" as a natural person who is a California resident, however identified, including by any unique identifier. *Id.* § 1798.140(g). In turn, "resident" means (1) every individual who is in California for other than a temporary or transitory purpose, and (2) every individual who is domiciled in California who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents. CAL. CODE REGS. tit. 18, § 17014 (2019).

[5] CAL. CIV. CODE § 1798.140(v).

[6] *Id.* § 1798.140(w).

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 [hereinafter GDPR].

[8] *See, e.g.*, CAL. CIV. CODE § 1798.110(a).

under the GDPR;[9] and (2) the right to request that a business delete the personal information the business has collected from them,[10] which is comparable to the "right to erasure" under the GDPR.[11]

Notwithstanding those similarities, ad-tech companies should carefully review any processes related to consumer access to or deletion of information they have implemented for GDPR compliance purposes and revise them as needed to meet the related, though not entirely co-extensive, requirements of the CCPA.

B. Scope of this analysis

This analysis will explain the rights California consumers have gained under the CCPA to request access to and deletion of their personal information, and how businesses are required to verify and respond to such requests. Further, it will provide recommendations to ad-tech companies regarding sensible approaches toward verifying and responding to such requests based on the text of the CCPA, industry best practices, and experience gained through the first year of compliance with the GDPR.

This analysis does not cover the full scope of the CCPA's requirements. For example, it does not provide guidance on changes businesses should make to their privacy policies for CCPA compliance, or how businesses should interpret requests from consumers to opt out of the sale of their personal information. Further, while this analysis does provide general explanations of certain CCPA provisions, it is not legal advice. All NAI members should consult with counsel to determine exactly how the CCPA applies to their specific business activities.

The NAI may update this analysis from time to time in order to reflect legislative or regulatory developments.

II. Consumer rights to access information under the CCPA

The CCPA grants California consumers the right to request that a business provide to them detailed disclosures about:

- The personal information the business has collected about them;
- Where the business got that information;
- The reasons why the business collected the information;
- To whom the business has disclosed that information, either by selling it or by sharing it for another reason.

This analysis refers to the above requests collectively as "Access Requests." Consumer rights to make Access Requests are discussed in more detail below.

[9] *See* GDPR, *supra* note 7, Art. 15.
[10] *See* CAL. CIV. CODE § 1798.105(a).
[11] *See* GDPR, *supra* note 7, Art. 17.

Requests for transparency into the personal information a business has collected about the consumer

With respect to personal information a business has collected about a consumer, the consumer has the right to request that the business disclose both (i) the categories of such personal information; and (ii) the specific pieces of personal information a business has collected about them.[12] In addition, a consumer has the right to request that the business disclose how it obtained such personal information, i.e., "the categories of sources" of the personal information.[13]

Requests for transparency into how the business shares personal information

If a business transfers personal information about a consumer to a third party, that consumer has the right to request that the business disclose the categories of third parties to which such information was disclosed.[14]

If the business's transfer of PI to a third party was a sale,[15] the consumer may also request that the business disclose the categories of third parties to which the business sold PI, matched to the categories of PI sold to each category of third party. However, if the business transfers that PI to another entity that is not a third party, and such transfer was made for a business purpose, the consumer has a right to request the categories of *PI* that were so transferred, but not the categories of *entities* to which such PI was transferred.[16] One example of a transfer of PI for a business purpose to an entity that is not a third party would be the transfer of such information to a service provider.

Requests for transparency into the business's purposes for processing personal information about the consumer

Consumers have the right to request that a business disclose to them any or all of the reasons why the business collects or sells personal information about them.[17] More specifically, a consumer may request disclosure specifying:

- The business purpose(s)[18] the business has for collecting the consumer's PI;
- The business purpose(s) the business has for selling the consumer's PI;

---

[12] *See* CAL. CIV. CODE §§ 1798.100(a); 1798.110(a); 1798.115(a)(1).
[13] *See id.* § 1798.110(a)(2).
[14] *See id.* § 1798.110(a)(4).
[15] The CCPA defines a "sale" as any "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," subject to several exceptions. *See id.* § 1798.140(t).
[16] *See id.* § 1798.115(a).
[17] *See id.* § 1798.110(a)(3).
[18] The CCPA defines "business purpose" to mean 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. It also enumerates a number of specific business purposes, including some that are specific to digital advertising, such as the contextual customization of ads,
counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards. *See id.* § 1798.140(d).

- The commercial purpose(s)[19] the business has for collecting the consumer's PI;
- The commercial purpose(s) the business has for selling the consumer's PI.

III. Consumer right to delete PI under the CCPA

In addition to the consumer rights to access PI (and related information) discussed above, the CCPA gives a consumer the right to request that a business delete any personal information the business has collected from the consumer, subject to certain qualifications and exceptions (hereinafter "Deletion Requests").[20] Furthermore, the business must direct its service providers to delete personal information related to a verified consumer request.[21]

IV. Duties of a business when receiving and responding to Access or Deletion Requests

Corresponding to the new rights granted to consumers by the CCPA to issue Access or Deletion Requests to businesses, businesses in turn have obligations under the CCPA regarding how to accept, verify, and respond to those Requests.

A. Methods for accepting Access and Deletion Requests

The CCPA requires all businesses to provide two or more methods consumers can use to submit, and through which the business can accept, Access and Deletion Requests.

Currently, the submission methods a business is required to make available to consumers are:[22]

- A toll-free phone number;[23]

[19] In contrast to "business purposes," the CCPA defines "commercial purposes" as those meant to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism. *See id.* § 1798.140(f).

[20] *See id.* § 1798.105(a). The qualifications and exceptions pertaining to Deletion Requests are explained in Section IV.C *infra.*

[21] *See* CAL. CIV. CODE § 1798.105(c).

[22] *See id.* § 1798.130(a)(1).

[23] A bill that would remove the requirement to provide a toll-free telephone number in certain limited circumstances has passed the California legislature and is expected to be signed into law by the Governor. *See* A.B. 1564, 2019-2020 Leg. Sess., Reg. Sess. (Ca. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1564. Assuming this amendment becomes law (as is expected), it is not clear that NAI members would be relieved of the obligation to make a toll-free telephone number available to consumers for making Access and Deletion Requests, because NAI members in many cases do not have "a direct relationship" with the consumer as required to qualify for the exception. If NAI members ultimately are required to accept Access and Deletion Requests via telephone, they should carefully consider special verification issues that may arise in that context. For example, it may be difficult to verify whether a consumer calling the toll-free number is the individual associated with a cookie ID or mobile ad ID maintained by

- A Web site address (if the business maintains an Internet Web site).

All NAI members maintain Internet Web sites, so they may consider using a web portal to satisfy the requirement to provide a Web site address where consumers may submit Access and Deletion Requests. If such a portal is also capable of receiving other consumer inquiries, it may also satisfy the requirements of the NAI Code of Conduct.[24]

In addition to the submission methods required by the CCPA, businesses may consider providing consumers with other convenient ways to submit Access or Deletion Requests. For example, most NAI members already maintain and monitor an email account for consumer inquiries.

B. Considerations for verifying Access and Deletion Requests

1. In general

The CCPA only requires businesses to act on an Access or Deletion Request if the request is a "verifiable consumer request."[25] Based on that, and the CCPA's definition of the term "verifiable consumer request,"[26] a business is only obligated to respond to an Access or Deletion Request originating from:

- A consumer on their own behalf;
- A consumer on behalf of the consumer's minor child; or
- A natural person or a person registered with the California Secretary of State, and authorized by the consumer to act on the consumer's behalf.

In addition, a business is only required to respond to requests from the above parties when the business can reasonably verify the consumer in question is the consumer about whom the business has collected personal information.[27] Put another way, a business is not obligated to take the actions requested by a consumer through an Access or Deletion Request if the business cannot reasonably verify:

- That the consumer making the request is the consumer about whom the business has collected personal information; or
- That the person making the request is authorized by that consumer to act on such consumer's behalf.

What counts as a "reasonable" verification procedure may vary depending on the type of PI that is subject to an Access or Deletion Request.[28] For example, businesses will likely adopt more rigorous

---

the business. Providing instructions to inquiring consumers about how to verify their request through other media may be the most prudent use of the toll-free number. Businesses could, for example, provide instructions over the phone about how submit an access request online or by mail that would allow for more robust verification procedures. For more information on verifying consumer requests, *see* Section IV.B *infra*.

[24] *See* NETWORK ADVERTISING INITIATIVE, 2018 NAI CODE OF CONDUCT § III.C.2 (2018) [hereinafter NAI CODE OF CONDUCT], http://www.networkadvertising.org/sites/default/files/nai_code2018.pdf.

[25] *See* CAL. CIV. CODE §§ 1798.100(c), 1798.105(c), 1798.110(b), 1798.115(b).

[26] *See id.* § 1798.140(y).

[27] *See id*.

[28] A recent proposed amendment to the CCPA would clarify this point by allowing a business to "require authentication of the consumer that is reasonable in light of the nature of the personal information requested."

verification procedures before disclosing potentially sensitive PI to the person making the request to avoid inadvertently releasing the information to a party who is not authorized to receive it. A few particularly salient examples where more robust verification methods may be called for include:

- Responding to an Access Request by disclosing specific pieces of PI that, if disclosed to an unauthorized person, would trigger the CCPA's data breach provision and its accompanying private right of action.[29] Such personal information is the non-encrypted or non-redacted:[30]
    - First name or first initial and 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:
        - Social security number;
        - Driver's license number or California identification card number;
        - 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;
        - Medical information; or
        - Health insurance information.
- Responding to requests for "household" information. The CCPA specifically includes information related to households, not just particular consumers, in its definition of "personal information" subject to Access and Deletion Requests.[31] Information pertaining to a household might include a mailing address where more than one consumer resides, or an IP address assigned to multiple devices owned by different users in the same household. In these or similar circumstances, there is an increased risk that a business's response to an Access Request that includes household-level information could reveal personal information about other consumers in the household without their authorization. As such, companies may consider methods of verifying that all members of a household have consented to one household member's submission of an Access or Deletion Request that would reveal household-level PI. Businesses should also keep in mind that the CCPA contemplates scenarios where one consumer's exercise of CCPA rights could harm other consumers when it states that "the rights afforded to consumers and the obligations imposed on the business [by the CCPA] shall not adversely affect the rights and freedoms of other consumers."[32][33]
    - Other questions to consider when responding to Requests that involve household data:

A.B. 25, 2019-2020 Leg. Sess., Reg. Sess. (Ca. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB25. This amendment has passed the legislature and is expected to be signed by the Governor.

[29] *See* CAL. CIV. CODE §§ 1798.150, 1798.81.5(d)(1)(A).

[30] A recent proposed amendment to the CCPA would clarify such that only information that is non-encrypted *and* non-redacted could trigger the data breach provision. *See* A.B. 1355, 2019-2020 Leg. Sess., Reg. Sess. (Ca. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1355. This amendment has passed the legislature and is expected to be signed by the Governor.

[31] *See* CAL. CIV. CODE § 1798.140(o).

[32] *See id.* § 1798.145(j).

[33] A proposed amendment would clarify that the Attorney General may adopt additional regulations 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. *See* Cal. A.B. 1355. Should the Attorney General adopt such regulations, the NAI will update this analysis to reflect any additional guidance.

- How does your business associate data on its platform? Is it by IP Address, or by a separate identifier?
- Would your business have to build something to pull in disparate information tied to, e.g., mobile ad IDs, that may also be associated with the same IP address?
- Would additional disclosures help clarify whether a Request will only be fulfilled in connection with a specific browser or device, or in connection with an IP address across browsers or devices?

More generally, verification methods may vary based on what is most appropriate given: (i) the kind of technologies used to collect or maintain such information; (ii) the type of personal information collected; and (iii) the channel through which a consumer may make an Access or Deletion Request. For example, if a consumer submits an Access or Deletion Request to an NAI member that works exclusively with pseudonymous information such as cookie IDs, verification procedures may differ from those used by companies that process direct identifiers, such as email addresses.

To identify the consumer for purposes of responding to an Access Request, the business must associate the information provided by the consumer in the verifiable consumer request to any PI previously collected by the business about the consumer. However, businesses are not required to "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."[34] It is not clear precisely how to interpret this provision. It may not exempt businesses from providing pseudonymous information in response to a request if the business can reasonably verify that the consumer making the request is entitled to it (e.g., by reading a browser cookie and getting an affidavit); however, it arguably does not require a business to link pseudonymous PI to separate PI provided in a request made, e.g., by physical mail or email, if the business has not already matched those two identifiers.

Beyond the general considerations addressed above, data subject requests under the GDPR have furnished some NAI members with experience that may be useful about how to verify Access and Deletion Requests under the CCPA. Below are some examples based on such NAI member input.

2. Pseudonymous identifiers

In cases where a business only holds a consumer's PI tied to pseudonymous identifiers, such as cookie IDs or mobile ad IDs, a business may encourage consumers to make Access and Deletion Requests through the medium by which the pseudonymous identifier was originally collected. Doing so could allow the identifier to be read and verified programmatically by the business. For example:

- Making a browser-based mechanism available to consumers through which they may make a request, so that the cookie ID(s) set on the browser and associated with a consumer's PI can be programmatically read for verification purposes;
- Making a mobile app-based mechanism available to consumers to make a request from, so that the device's mobile ad ID associated with a consumer's PI can be programmatically read for verification purposes.

[34] CAL. CIV. CODE § 1798.110(d).

In cases where a cookie ID or mobile ad ID cannot be programmatically obtained, such as when the consumer is making a request from a device other than the one which stores the pseudonymous ID, businesses may consider providing consumers with instructions about how to obtain the pseudonymous ID through device settings, and how to then submit that ID manually. This could involve the consumer sending a screenshot of the pseudonymous ID, or providing a web-based mechanism where the pseudonymous ID may be entered manually and then submitted to the business.

Businesses that plan to accept Access or Deletion Requests for pseudonymous identifiers should also keep the following caveats in mind:

- Cookie ID attributes such as *name* and *value* can be tampered with in web browsers using JavaScript or developer tools. It is therefore technically feasible for individuals making Access or Deletion requests to adjust cookies on a web browser to match cookie IDs associated with a consumer whose PI they are not authorized to access.
- Screenshots can easily be tampered with or spoofed, so companies that intend to rely on screenshots may consider bolstering that process with additional verification or authentication procedures.
- The latest version of iOS does not display the device's ID for Advertising (IDFA) to a consumer in the device's settings. Therefore, to manually access the IDFA on iOS devices, consumers would likely need to install a third-party app, which would present its own privacy and security risks.
    - On Android devices, however, consumers can view the device's advertising ID (MAID) by navigating through Settings → Google (Services & preferences) → Ads.

3. Direct identifiers

In cases where a business holds PI that directly identifies a consumer, such as an email address or phone number, there are different considerations for verifying requests. For example, it may be possible for a business to send a verification message to the account associated with the PI in question (e.g., via email or text message), in order to verify that the consumer making the request controls the account the PI is associated with.

One method to prompt this kind of verification procedure would be to direct consumers to an online portal where they submit the identifier in question (e.g., their email address or telephone number). Then, the business's verification message could contain:

- A URL with a unique verification parameter, which the consumer can navigate to in order to authenticate their identity; or
- A verification code, which the consumer could subsequently enter into the online portal to authenticate their identity.

Businesses that plan to accept Access or Deletion Requests associated with direct identifiers should also keep the following caveats in mind:

- If using a URL as a means to authenticate identity in a verification email, consider ways to prevent bad actors from easily spoofing the URL parameters. For example, it would be relatively easy to spoof a unique parameter consisting of a consumer's email address in plaintext (e.g., https://adtech-company.com/email-verification?**email=john.smith%40test.com**). One way to

address this spoofing concern would be to encrypt the verification URL parameters and then decrypt them server-side following the consumer navigating to the URL so that the verification URL parameters are harder to spoof (e.g., https://adtech-company.com/email-verification?**email=g4h219saj29/ra**).

4. Other verification considerations

Some ad-tech companies may consider providing a real-time response to Access or Deletion requests when they can do so programmatically (e.g., reading a cookie ID and immediately returning information associated with that cookie ID through a web portal). However, in cases where a business is not capable of responding to an Access or Deletion request in real time following successful verification, that business should consider how it will provide the required information to consumers at a later time. Examples include:

- Providing the consumer with a URL where the requested information will be posted at a later time;
- If a business holds directly identifying PI related to a consumer (such as an email address, phone number, or physical address), the business may send the required information (or a URL where it can be accessed), to the consumer through those avenues at a later time;
- Requesting contact information, such as an email address, phone number, or address, where the required information (or a URL where it can be accessed) can be sent to the consumer at a later time;
- If a business maintains pseudonymous identifiers associated with internet-connected devices such as smart TVs or other IoT devices, the same considerations apply as with the mobile and web context. If a business is in a position to do so, it could read and verify those identifiers programmatically. Otherwise, it may allow for the manual submission of the identifier via screenshot or entry of the identifier's value through a separate web portal.

Further, businesses may consider using, in addition to technical measures like the ones described above, other methods to verify a consumer's Access or Deletion Request. Such additional steps could include:

- Requiring the submission of an affidavit representing the truth of the relevant facts (e.g., that the affiant is the owner of the email address, or the device through which a request is being submitted);
- Requiring the submission of a notarized form;
- Requiring the submission of a copy of a government-issued identifier, such as a driver's license or passport.
    - If a company asks for government issued identification or other forms of PI it would not normally collect, the company should be prepared to take steps to secure this information related to verification, and/or institute processes to delete the PI after verification has been completed.

Businesses should not provide any PI to a consumer or delete any PI in response to an Access or Deletion request unless such action is pursuant to a verifiable consumer request. Put another way, businesses should not forego reasonable verification procedures when responding to requests.[35]

[35] *See id.* § 1798.100(c)

Business should also keep in mind that the CCPA anticipates that the California Attorney General will issue regulations governing verification procedures.[36] The NAI will update this analysis when those regulations become available, as necessary.

Finally, a recent proposed amendment clarifies that the CCPA 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." The amendment has passed the California legislature and it is expected that the Governor will sign the amendment into law.[37] This provision may be useful to businesses weighing whether to collect additional information to verify a consumer request or deny the request because it is not a verifiable consumer request in relation to the PI the business has already collected about a consumer.

C. Denying Access or Deletion Requests

If a business does not take the actions requested by a consumer through an Access or Deletion Request for a permissible reason, the business is still obligated to inform the consumer making the request of the reasons why it is not taking any of the actions requested by the consumer, and must provide any appeal procedures the consumer may engage in.[38] That means businesses must be prepared to collect whatever information may be necessary to contact the consumer regarding that consumer's Access or Deletion Request at the time the request is made. If a business plans to respond to requests programmatically in real-time, this may not present an issue, but if a business expects any delay when processing a request, the business should consider how it will communicate any eventual denial of a request to the consumer.[39] This could be a particular concern for businesses that are required to field consumer requests through a toll-free telephone number. Below are circumstances where a business may refuse to act on an Access or Deletion Request:

- A business may refuse to act on a consumer's Access Request if the business is unable to verify that they are the consumer about whom the business has collected personal information.[40] This situation could arise, for example, if the consumer did not take all of the steps required by the business to reasonably verify the request, or if the business is unable to verify the request after going through its own reasonable verification procedures.
- A business may refuse to act on an Access or Deletion request if such a request from a consumer is manifestly unfounded or excessive, in particular because of its repetitive character. In this case, however, the business bears the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.[41]
- A business may deny a consumer's Deletion Request, even if the request is a verifiable consumer request, if it is necessary for the business (or a service provider of the business) to retain the PI subject to the request in order to:[42]

[36] *See id.* § 1798.185(a)(7).
[37] A.B. 1355, 2019-2020 Leg. Sess., Reg. Sess. (Ca. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1355.
[38] *See* CAL. CIV. CODE § 1798.145(g).
[39] The timing of this response to consumers is governed by the same requirements articulated in Section IV.E *infra*.
[40] *See* CAL. CIV. CODE § 1798.140(y).
[41] *See id.* § 1798.145(g).
[42] *See id.* § 1798.105(d).

- Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- Debug to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
- 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.
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.
- To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
- Comply with a legal obligation.
    - For example, if a business's records (which may include a consumer's PI) are subject to discovery in litigation or in a regulatory matter, the business may be legally obligated to suspend any deletion or destruction of records that are relevant to the matter to avoid spoliation of evidence.
- 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.
    - While this exception may appear to support a broad exception to Deletion Requests, the NAI would not support using this exception to retain a consumer's PI for interest-based advertising purposes after receipt of a Deletion Request.

For each category of exception above, the business is still required to respond to the consumer in a timely manner to provide the reasons why it will not grant the Request for Access or Deletion, as well as provide the steps, if any, the consumer may take to appeal the business's decision.

D. Form of response to Access and Deletion Requests

After a business has (i) received a Request for Access or Deletion; (ii) determined that it is a verifiable consumer request; and (iii) determined there are no other grounds on which it will refuse to act on the Request, there are still numerous requirements it must meet when acting on those Requests. The specific requirements may vary depending on the content of the Request.

1. Deletion requests

When a business acts on a Deletion Request, it must (i) delete the consumer's PI from its records; and (ii) direct its service providers to delete the consumer's PI from their records.[43]

[43] *See id.* § 1798.105(c).

However, the plain language of the statute suggests that this consumer right applies only to information a business has "*collected from the consumer*," and so may not extend to PI a business has not collected directly from the consumer (e.g., PI received from another business or a third party).[44] Still, businesses should take care to be internally consistent about how they are characterizing the source of PI they are processing. For example, some ad-tech companies may conclude that they do not collect consumer PI from third parties because their technology collects information directly from a consumer (or the consumer's browser or device) by observing that consumer's behavior. But in that case, such PI would more clearly be subject to consumer Deletion Requests. Conversely, if an ad-tech company determines that the way its technology integrates with a publisher's mobile app or web site *does* constitute a transfer of PI by the publisher to the ad-tech (e.g., if it is a "sale"), then arguably the ad-tech company is not required to act on a Deletion Request because it did not collect the information from the consumer, but rather from another business or third party.

In some cases, that may mean that a business receiving a Deletion Request would be required to delete (or direct its service provider(s) to delete) only some of the PI it holds about a consumer. This would also be the case if an exception applied to the Deletion Request, but only with regard to some of the PI at issue.[45]

2. Access requests

Businesses that receive a verifiable consumer request for access to PI, and related information (such as purposes for collecting it), have to meet a number of requirements as to how and when they respond to the consumer making the request.

For all responses, the information provided by a business in response to an Access Request must be in writing, and in a form that is "reasonably accessible to the consumer."[46] Further, if the consumer maintains an account with the business, the business must deliver the information through the consumer's account.[47] On the other hand, if the consumer does not have an account with the business, the information may be delivered by mail or electronically, at the election of the consumer.[48] If provided by the business electronically, the information must be in a format that is portable, and, to the extent technically feasible, readily useable such that it allows the consumer to transmit the information to another entity without hindrance.[49]

As many NAI members do not have a direct relationship with consumers, and hence do not have consumers who maintain accounts tied to direct identifiers such as name, email address, or phone number in the ordinary course of business, these member companies may not be required to deliver information through a consumer account (because they do not maintain consumer accounts). And,

[44] The CCPA defines "collect" broadly as "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." *See id.* § 1798.140(e). As such, business should avoid interpreting the PI they "collect" from consumers too narrowly. It clearly covers more than information a consumer has actively submitted to a business.
[45] *See* Section IV.C *supra*.
[46] *See* CAL. CIV. CODE § 1798.130(a).
[47] *See id.* § 1798.130(a)(2).
[48] *See id.*
[49] *See id.* § 1798.100(d).

while some businesses may prefer to have consumers create accounts with them to ease the verification process, they may not *require* the consumer to create an account in order to make a verifiable consumer request.[50] Businesses may be able to offer account creation as an alternative way for consumers to receive PI in response to Access Requests, so long as other methods are also offered. That said, many NAI members deal only with pseudonymous information and would prefer to avoid collecting or processing direct identifiers, even if only for verification purposes, and the CCPA does not require businesses to provide account creation as an alternative verification procedure.

The requirements below distinguish between businesses that "collect" PI, businesses that "sell" PI, and businesses that discloses PI for a "business purpose."

Businesses that "collect" PI

Because the definition of "collect" is quite broad, it likely covers some aspect of all NAI members' business activities. Specifically, the CCPA defines "collect" to include "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."[51] Additionally, it does not appear to be possible for a business to "sell" PI or disclose PI for a "business purpose" unless that business has already "collected" the PI to be sold or otherwise disclosed.

When a business that collects PI is determining how to respond to a consumer's Access Request, it should keep in mind that consumers may request more than just the specific pieces of PI the business holds about them. Consumers also have the right to request (i) the categories of such PI;[52] and (ii) the categories of sources from which the business obtained such PI.[53]

When compiling the categories of PI for disclosure to a consumer in response to an Access Request, businesses must follow the CCPA's definition of PI and reference the enumerated category or categories therein that most closely describe the PI.[54] The categories of PI included in the CCPA's definition are:[55]

- 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.
    - A **unique personal identifier** is 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

[50] *See id.* § 1798.130(a)(2).
[51] *Id.* § 1798.140(e).
[52] *Id.* § 1798.110(a)(1).
[53] *Id.* § 1798.110(a)(2)
[54] *Id.* § 1798.130(a)(4), (c).
[55] *See id.* § 1798.140(o).

particular consumer or device. In this context, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.[56]
    - A **probabilistic identifier** is 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.[57]
- Any categories of personal information described in subdivision (e) of Section 1798.80 of the California Civil Code.
    - This includes name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.[58]
- Characteristics of protected classifications under California or federal law.
    - For example, classifications based on race, religion, sex, disability, and many other characteristics are protected classifications under various California or federal laws.
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (FERPA).[59]
- 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.

The CCPA does not specify how to list the "categories of sources" of PI to be used in response to an Access Request, but these might include categories such as PI provided by the consumer, PI obtained from public records, PI collected automatically (e.g., through cookies and SDKs), and PI shared by business partners, among other categories.

All businesses that collect PI are required to disclose the categories of third parties,[60] if any, with whom they *share* PI in response to an Access Request for that information.[61] This requirement does not appear to be limited to "sales" of PI. The CCPA does not give specific guidance as to classifying different categories of third parties, but ad-tech companies may consider using accepted industry classifications

[56] *Id.* § 1798.140(x).
[57] *Id.* § 1798.140(p).
[58] *See id.* § 1798.80(e).
[59] 20 U.S.C. § 1232g; 34 C.F.R. §§ 99.1–99.67.
[60] The CCPA defines "third party" in such a way as to generally exclude service providers. *See* CAL. CIV. CODE § 1798.140(w).
[61] *See id.* § 1798.110(c)(4).

for categories of businesses like SSP, Exchange, DSP, Data Aggregator, Identity Solution Provider, Ad Server, Analytics Provider, etc.

Finally, businesses that collect PI must disclose in response to an Access Request the business and/or commercial *purpose(s)* for any collection (or sale) of PI.[62] In responding to such a request, businesses may consider mirroring the enumerated purposes found in the definition of "business purpose," to the extent applicable.[63] Also note that "commercial purposes" for the collection (or sale) of PI, which also must be disclosed in response to an Access Request for the same, are defined separately from "business purposes."[64]

Businesses that sell PI or share PI for a business purpose

Businesses have an obligation under the CCPA to disclose information about the PI they transfer to other entities, and the categories of entities to which the PI is transferred, in response to an Access Request for that information. As explained below, these obligations vary based on whether the transfers at issue are CCPA "sales."

A business that *sells* PI, when responding to a consumer's verified Access Request regarding PI the business has sold, must (1) identify the PI about the consumer that it has sold in the preceding 12 months, by the category or categories that most closely describes the PI (see the list of categories in the definition of PI above); and (2) provide the categories of third parties to whom it sold the consumer's PI in the preceding 12 months by reference to each such category of PI. The business shall disclose this information in a separate list.[65]

Example:

Categories of Third Parties to Whom PI Was Sold in the 12 months preceding the request	**Categories of PI Sold to that Category of Third Party (by categories enumerated in the definition of PI)**
Data aggregator	Browsing history Geolocation data Inferences drawn to create a profile reflecting consumer interests
DSP	Internet or other network activity information IP Address Online Identifiers
...	...

A business that discloses PI to another entity *for a business purpose* must (1) identify the PI about the consumer that it has disclosed for a business purpose in the preceding 12 months, by the category or

[62] *See id.* §§ 1798.110(a)(3), 1798.115(a)(3).
[63] *See id.* § 1798.140(d).
[64] *See id.* § 1798.140(f).
[65] *See id.* §§ 1798.115(c)(1), 1798.130(a)(4)(B)–(C).

categories that most closely describes the PI (see the list of categories in the definition of PI above); and (2) provide the categories of third parties to whom it disclosed the consumer's PI for a business purpose in the preceding 12 months by reference to each such category of PI. The business must disclose the information in a separate list.[66]

Example:

Categories of Third Parties to Whom PI Was Disclosed for a Business Purpose in the 12 months preceding the request	**Categories of PI Disclosed for a Business Purpose to that Category of Third Party (by category of PI enumerated in the definition PI)**
Exchange	Internet or other network activity information IP Address Online Identifiers
Analytics provider	Internet or other network activity information IP Address Online Identifiers Consumer interaction with a web site
…	**…**

3. Lookback requirements

The disclosure provided by a business to a consumer in response to an Access Request must cover the 12-month period preceding the business's receipt of the verifiable consumer request.[67]

There has been some concern about whether this requirement in the CCPA is intended to force businesses to, e.g., change an existing 30-day retention policy to 12 months in order to properly respond to an Access Request. But such an interpretation of the requirement would be inconsistent with good data minimization practices, and there is some support in the statutory language that extending data retention policies is not required for this purpose. For example: "This section does not require a business to . . . [r]etain 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."[68] Further, a proposed amendment would clarify that the CCPA shall not be construed to require a business to "retain personal information for longer than it would otherwise retain such information in the ordinary course of its business."[69] This amendment has passed the California legislature and is expected to be signed into law by the Governor.

[66] *See id.* §§ 1798.115(c)(2), 1798.130(a)(4)(B)-(C).
[67] *Id.* § 1798.130(a)(2)
[68] *Id.* § 1798.110(d).
[69] Cal. A.B. 1355.

4. Charging a fee for responding to requests

If a business receives a verifiable Access Request, the business must promptly take steps to disclose and deliver, *free of charge to the consumer*, the PI (and associated information) required by the CCPA.[70]

However, if requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may charge a reasonable fee, taking into account the administrative costs associated with responding to the request. Still, businesses should exercise caution before seeking to charge a fee when responding to such a request, as the business bears the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.[71]

E. Frequency and timing of responses

1. Frequency of responses

There is no limit on how many times a business *may* provide PI to a consumer in response to verified requests, but the CCPA does not require the business to provide PI in response to a verified request more than twice in a 12-month period.[72] However, businesses should be cautious if they intend to decline requests to provide PI more frequently that twice in a 12-month period, because they are still required to respond to the request with the reason why the request was not fulfilled in a timely manner. Further, businesses should consider if this limitation on responses applies only to the specific pieces of PI they hold about a consumer, or if it extends to related information such as the categories of sources of that information. The CCPA is silent on this point, but note that the language of the limitation refers explicitly only to the provision of "personal information," not to categories of sources, etc.

2. Timing of responses

Upon receipt of a verified consumer request, a business must disclose and deliver the required information to the consumer free of charge within 45 days of receipt of the request. Notwithstanding the 45-day response period, a business must, in each case, promptly take steps to determine whether the request it has received is a verified consumer request. Note that the 45-day period begins tolling upon the business's *receipt* of the request, not upon the time that the business determines whether the request is a verifiable consumer request. A business may extend the initial 45-day response period by one additional 45-day period, but only when:

- Additional time to verify or process the request is reasonably necessary;
- The business notifies the consumer making the request within the initial 45-day window of the fact that it is taking the extension.[73]

[70] CAL. CIV. CODE § 1798.100(d).
[71] *See id.* § 1798.145(g).
[72] *See id.* §§ 1798.100(d), § 1798.130(b).
[73] *See id.* § 1798.130(a)(2).

Further, a business may elect to extend its time to respond to a request by up to 90 days, instead of 45, but only when *necessary*, taking into account the complexity and number of the requests the business is processing. The CCPA does not elaborate on when a 90-day extension may be "necessary" over and above when a 45-day extension may be "reasonably necessary." Still, when a business does elect to take a 90-day extension, the business still must notify the consumer making the request within the initial 45-day window of the fact that it is taking the 90-day extension, along with the reasons for delay.[74]

The CCPA does not appear to require that a business seek approval from a consumer or a regulator before taking an extension, however businesses generally should consider documenting and being able to demonstrate the validity of the reasons why an extension was taken.

F. Service providers

A business that receives a verifiable Deletion Request from a consumer must direct any service providers processing that consumer's PI on its behalf to comply with the Deletion Request.[75] Conversely, when a company is acting as a service provider for a business, it must comply with that business's direction to delete PI in response to a verifiable Deletion Request. The CCPA is silent on a service provider's obligations with respect to Access Requests, but companies acting as service providers to a business generally should seek to cooperate with and honor Access and Deletion Requests passed on by that business.

Businesses that pass Deletion Requests on to their service providers may be concerned about their service providers' compliance with such requests. While the CCPA is silent on the specific issue of liability for a service provider's failure to comply with a Deletion Request, the CCPA does contain a general limitation on businesses' liability when they rely on their service providers in good faith:

> A business that discloses personal information to a service provider shall not be liable under [the CCPA] if the service provider receiving the personal information uses it in violation of the restrictions set forth in [the CCPA], 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[.][76]

Companies acting as service providers may similarly be concerned about whether they are required to verify and/or respond to Access or Deletion Requests independently of the business on whose behalf they are processing PI. Again, the CCPA is silent on this specific issue, but companies acting as service providers may consider how the following carve-out for service provider obligations applies to their specific business relationships:

> A service provider shall likewise not be liable under [the CCPA] for the obligations of a business for which it provides services as set forth in [the CCPA].[77]

---

[74] *See id.* § 1798.145(g).
[75] *Id.* § 1798.105(c).
[76] *Id.* § 1798.145(h).
[77] *Id.*

Still, if a service provider receives an Access or Deletion Request directly from a consumer, it may consider asking the consumer to submit her request to the business for which it is acting as a service provider, or forwarding the request to that business. However, companies should confirm first that they are not processing any of that consumer's PI in their own capacity as a business, even if they are acting as a service provider to other businesses with respect to the same consumer's PI. Companies must comply with their own obligations as a "business" under the CCPA, including responding to Access and Deletion Requests, even if they are acting as service providers in some contexts or with some business partners.

G. Hypothetical scenarios for NAI members to consider when responding to Access or Deletion Requests

A number of NAI members have substantial experience responding to data subject requests made under the GDPR. They have generously shared some hypothetical scenarios to consider based on and abstracted from that experience:

- If a consumer makes an Access Request to a business that only uses cookie IDs, but the consumer has recently cleared cookies (so the business has no way to match the consumer), consider whether that means the company has no PI about the consumer.
    - In this scenario, the business may still have a unique ID stored server-side that would be considered PI. The fact that the business does not have a direct way to match or verify it does not entail that the company has no PI.
    - A similar scenario arises when a company has opted out a consumer by zeroing out the cookie ID.
- Anticipate, and have preliminary responses vetted and prepared, for questions such as "How do you know that's all of the PI you have about me?"
    - Consumers posing such questions may be insinuating that a company is being dishonest, so thoughtful responses to such questions are appropriate.
    - The response may also implicate what the company thinks is in scope for the request, which is something a consumer may be "testing."
- Anticipate detailed questions about the categories (and identities) of third parties with whom the business shares PI. Also consider whether a business should forward requests to other companies when a consumer asks the business to do so.
- When responding to a Deletion Request, how will a business confirm it deleted all PI that was in-scope for the request? Is there data on one table that links to another that was not deleted? How can a business demonstrate or confirm this?
    - If a business anticipates that its primary fact table will be in-scope (e.g., a UID database), but there are derived tables created ad hoc or for specific purposes, consider whether mechanisms for responding to requests account for those.

V. Recommendations

- Determine whether you are a "business," "service provider," or "third party" in relation to the consumer making the request.[78]
- Create written policies and procedures to address the following:
    - What consumer request mechanisms will be maintained, and how they will be monitored.
    - Verification procedures for responding to consumer requests, taking into account how the request is made and what kind(s) of PI the company maintains.
    - The timing required for execution of verification and response procedures, and when to notify consumers that the company is taking an extension.
    - Accepting and responding to consumer complaints or appeals based on an initial response.
- Assign individual(s) responsibility for accepting and responding to requests.
- Provide appropriate training to personnel that may receive consumer requests in different channels.[79]
- Document and maintain records of all consumer requests, how and when the request was received, and how the business responded (audit trail).
- Map data against required PI categories to provide accurate and thorough responses.
    - This should include documenting the purposes for which each type of PI is collected or sold.
    - Review vendor and customer lists, and assign categories to each entity on those lists (to meet requirement to disclose categories of third parties to whom PI is sold or disclosed for a business purpose).
- Consider developing additional policies and procedures for processing requests made by a consumer's authorized agent designed to minimize the risk of inadvertent or unauthorized disclosure of PI.
    - This is a particular concern for PI that could trigger the CCPA's data breach provisions,[80] which is subject to a private right of action.

[78] The NAI's CCPA Implementation Working Group is analyzing this issue and may issue guidance on it in the future.
[79] 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 . . . [e]nsure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Sections 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections. CAL. CIV. CODE § 1798.130(a)(6).
[80] *See id.* § 1798.150.