409 7th Street, NW Suite 250
Washington, DC 20004

Submitted via email to: databrokers@cppa.ca.gov

June 25, 2024

California Privacy Protection Agency
Data Broker Unit
2101 Arena Blvd
Sacramento, CA 95834

Re: NAI Response to Invitation for Preliminary Comments on Proposed Rulemaking under SB 362

To the CPPA Data Broker Unit:

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to provide preliminary comments on the California Privacy Protection Agency's ("Agency") proposed rulemaking to implement the Data Broker Delete Requests and Opt-Out Platform ("DROP").

Founded in 2000, the NAI is the leading non-profit, self-regulatory association for advertising-technology companies. For over 20 years, the NAI has promoted strong consumer privacy protections, a free and open internet, and a robust digital advertising industry by maintaining the highest industry standards for the responsible collection and use of consumer data for advertising. Our member companies range from large multinational corporations to smaller startups and represent a significant portion of the digital advertising technology ecosystem, all committed to strong self-regulation and enhancing consumer trust.

A significant part of the NAI membership is also represented on California's data broker registry and has a keen interest in seeing the DROP implemented in a way that meets the intent of SB 362 while minimizing the burdens on both consumers using the DROP and registered brokers integrating with it.

Our comments below follow the structure of the Agency's prompts in its request for comments (RFC), and are organized as follows:

I. Verifiable Consumer Requests

A. CPPA Prompt:

"The Delete Act requires the Agency to establish an accessible deletion mechanism that allows a consumer, through a "verifiable consumer request," to request every data broker that maintains any non-exempt personal information about them to delete that personal information. a. What should constitute a "verifiable consumer request"? b. For data brokers, how does your company currently verify CCPA requests to delete? What information is necessary for the verification process? What challenges do you face in verifying consumers? c. For consumers, what has been your experience with submitting verifiable consumer requests under the CCPA to businesses, including data brokers? Are there verification processes that you have preferred over others?"[1]

B. NAI Responses:

1. *General Background on Statutory and Regulatory Framework for the DROP*

As the Agency deliberates about what should constitute a "verifiable consumer request" for purposes of the DROP, the Agency should, as a threshold matter, look to the existing statutory and regulatory context found in the CCPA, its implementing regulations, and the Delete Act itself.

[1] California Privacy Protection Agency, Invitation For Preliminary Comments On Proposed Rulemaking Under Senate Bill 362 (May 31, 2024) (hereinafter "Request for Comments" or "RFC"), https://cppa.ca.gov/regulations/pdf/invitation_for_comments_drop.pdf.

As the Agency noted in its RFC, the Delete Act requires the Agency to:

> "establish an accessible deletion mechanism that . . . [a]llows a consumer, ***through a single verifiable consumer request***, to request that every data broker that maintains any personal information delete any personal information related to that consumer held by the data broker or associated service provider or contractor."[2]

"Verifiable consumer request" is not defined by the Delete Act; however, the Delete Act does provide that "[t]he definitions [of the CCPA] shall apply unless otherwise specified in this title."[3] It appears, then, that the Delete Act requires the Agency to look to the CCPA's definition of "verifiable consumer request"[4] when determining how the Delete Act requires the DROP handle those requests.

The CCPA defines "verifiable consumer request" as follows:[5]

> "[A] request that is made by a consumer, by a consumer on behalf of the consumer's minor child, by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, or by a person who has power of attorney or is acting as a conservator for the consumer, and that the business can verify, using commercially reasonable methods . . . to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115, to delete personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, if the business cannot verify . . . that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf."

Notably, the CCPA's definition of a verifiable consumer request (or "VCR") refers to a request between two parties: the request must be made *by a consumer* (or in certain cases by another person on behalf of the consumer) and must be capable of being verified by *the business* using commercially reasonable efforts. This structural feature of the CCPA definition of VCR creates a degree of tension with the Delete Act's mandate that the Agency mediate requests between those two parties through the DROP. More specifically, the Agency does not appear to be eligible to "verify" a consumer's request or act as the recipient of VCR under the CCPA or the

[2] CAL. CIV. CODE § 1798.99.86(a)(2) (emphasis added).
[3] *Id.* § 1798.99.80(a).
[4] *Id.* § 1798.140(ak).
[5] *Id.*

Delete Act – only a "business" can play that role. On the other hand, if the Agency does not play a role in authenticating the individuals using the DROP and normalizing VCRs made available to registered brokers through it, the DROP's functionality to consumers will be severely hindered.

As discussed in the following section below, the NAI identifies two potential paths the Agency could take in developing the DROP, and we recommend that the Agency take the second path ("Path 2") by playing a role in *authenticating* individuals seeking to make VCRs before making those requests available to brokers through the DROP, while enabling registered brokers to *verify* those VCRs after they are accessed through the DROP.

> *2. The Agency has at least two potential design paths to choose between while developing the DROP; and should take the path that puts the responsibility for authenticating individuals seeking to submit VCRs on the Agency before those VCRs are accessed by brokers.*

As discussed above, the Delete Act requires the DROP to enable all registered data brokers to access and process a single VCR made by a consumer. From the NAI's perspective, there are two potential paths the Agency could take in fulfilling this requirement that vary based on the role the Agency plays in authenticating the "single" VCR[6] submitted by an individual.

As set out in more detail below, the NAI believes the Agency should follow Path 2 and take responsibility for authenticating an individual seeking to submit a VCR through the DROP *before* the DROP makes that request available to registered data brokers. It should do so by recognizing an important distinction between: (1) *authenticating* that an individual seeking to submit a VCR through the DROP is a California "consumer" eligible and intending to make that request; and (2) the *verification* of the request by registered brokers. Because of the difficulties presented by Path 1 for both consumers and registered brokers, the NAI recommends that the Agency pursue Path 2. The NAI is hopeful that the Agency can use its rulemaking authority under the Delete Act[7] to implement Path 2 in a way that is consistent with the CCPA and the Delete Act's statutory requirements[8] by relying on the distinction between authentication and verification.

[6] *Id.* § 1798.99.86(a)(2).
[7] *See id.* § 1798.99.87(a).
[8] *See id.* § 1798.99.88.

a. Path 1: No Agency role in authenticating individuals seeking to use the DROP.

Under Path 1, the Agency could design the DROP to allow an individual to make a single request to delete through the DROP, after which the DROP would make that unauthenticated and unverified request available to registered brokers to process individually. Because the Agency would not play a role in authenticating the individual attempting to make VCR under Path 1, each registered data broker would have to treat the individual's request received through the DROP as if it were submitted directly to the registered broker and subject the request to the same authentication and verification processes the broker would otherwise use for such requests. In some ways, Path 1 may represent a simpler and easier-to-administer process from the Agency's perspective. However, it would involve significant drawbacks for both California consumers and registered brokers.

From the consumer perspective, using the DROP before *authenticating* their status as a California consumer (and their control over the identifiers they wish to submit) would likely trigger an independent authentication process from each registered broker. Currently, nearly 500 separate businesses are registered as data brokers in California.[9] That means a consumer submitting a request through the DROP would have to interact with nearly 500 businesses and undergo distinct and non-uniform authentication processes for each of them (for example, responding to nearly 500 authentication emails, confirmation text messages, or other similar steps). This level of friction and administrative burden on consumers using the DROP would make it difficult for them to complete their requests (we will refer to this difficulty throughout our comments as the "**Individualized Consumer Authentication Problem**").

From the registered broker perspective, going through full authentication and verification procedures for a higher volume of requests to delete from the DROP – in addition to those already received through, *e.g.*, their websites – would involve a greater administrative burden as well. This, along with the potential for inconsistent authentication methodologies and results, could also lead to frustration from consumers.

b. Path 2: The Agency takes responsibility for authenticating individuals seeking to use the DROP.

Under Path 2, the Agency would play a central role in authenticating an individual seeking to submit a request through the DROP by confirming that the individual: (1) is a California

[9] *See* California Privacy Protection Agency, *Data Broker Registry*, https://cppa.ca.gov/data_broker_registry/ (last visited June 25, 2024).

"consumer" eligible to make the request;[10] and (2) has ownership or control over the identifiers the individual is submitting in connection with the deletion request.

If the Agency can successfully *authenticate* those two items, it would enable registered brokers to rely on the Agency's determination that the request at issue is an authentic VCR before those brokers individually *verify* whether the authenticated consumer making the VCR is the consumer "about whom" registered data brokers may have collected information pursuant to the CCPA definition of VCR.[11] The NAI believes that in many (if not all) cases, this type of *verification* by brokers can be achieved without any further need to communicate with the requestor, because if the Agency has already *authenticated* the request and associated identifiers, then a registered broker only needs to seek a match for those authenticated identifiers within its data product(s). If a match is found, the broker should treat the VCR as verified (*i.e.*, the match would confirm that the request relates to a consumer "about whom" the broker has collected information based on the matched identifier(s)). If no match is found, then the broker may conclude that it cannot verify that the request relates to a consumer about whom they have collected personal information, deny the deletion request, and instead process the VCR as an opt-out request as required by the Delete Act.[12]

Path 2 offers obvious advantages to both consumers and registered data brokers compared to Path 1. From the consumer perspective, it would greatly reduce the workload and friction consumers could expect from submitting an unauthenticated request to delete through the DROP, thus avoiding the **Individualized Consumer Authentication Problem.** In addition, from the perspective of registered brokers, relying on the Agency to authenticate consumers before making their requests available through the DROP would ease the burdensome and time-consuming authentication processes they would otherwise be met with due to any increase in request volume from the DROP. Therefore, the NAI recommends that the Agency opt for Path 2 in its development of the DROP.

However, the NAI is mindful that following Path 2 requires carefully distinguishing the *authentication* of an individual seeking to use the DROP by the Agency from *verification* of the VCR by registered brokers. The Agency is not authorized to *verify* consumer requests, because the definition of "verifiable consumer request" the Agency is required to adhere to in implementing the DROP, as discussed above in Section I.B.1., refers to consumer requests made by a consumer to a *business*, and that the business is generally the entity responsible for verifying those requests. "Business" is not defined by the Delete Act but is defined by the

[10] *See* CAL. CIV. CODE §§ 1798.99.86(a)(2); 1798.140(i).
[11] *See* CAL. CIV. CODE § 1798.140(ak).
[12] *See id. §* 1798.99.86(c)(1).

CCPA.[13] The Agency does not meet the CCPA's definition of a "business" and is not the entity that has "collected information about the consumer," which seems to preclude the Agency from verifying the requests.[14] The Delete Act also explicitly contemplates registered brokers denying deletion requests if "the request cannot be verified" by the broker,[15] which would be vacuous if the Agency were solely responsible for *verifying* requests made available through the DROP.

3. If following Path 2, the Agency should develop a robust authentication procedure for individuals submitting requests through the DROP that registered brokers can safely rely on and that prevents abusive or fraudulent requests.

For the reasons discussed above, the NAI believes the Agency should follow "Path 2" in designing the DROP by taking responsibility for properly authenticating consumer requests to delete submitted through the DROP *before* making those requests available to registered data brokers to act upon. However, if the Agency takes Path 2, it is imperative that the authentication procedures it puts into place are robust and effective in order to ensure the following two criteria are met: (1) as required by the Delete Act, that only "consumers" (*i.e.*, California residents) entitled to use the DROP are able to submit requests through it;[16] and (2) to maintain the integrity of the DROP, prevent it from becoming a vector for inauthentic or fraudulent requests to delete (*i.e.*, deletion requests that are not generated at the intent of any specific California consumer, or relate to identifiers that the consumer owns or controls). The NAI has several recommendations for implementing such authentication procedures, discussed in turn below.

a. The Agency should ensure that only California residents can use the DROP.

The Delete Act makes clear that the DROP should support VCRs from "consumers"[17] and that brokers are only required to honor requests made by "consumers."[18] The Delete Act does not define "consumer," but the CCPA does, as follows:

> "a natural person who is a California resident . . . however identified, including by any unique identifier."[19]

[13] *See id.* § 1798.140(d).
[14] *See id.*
[15] *See id.* § 1798.99.86(c)(1)(B).
[16] *See id.* §§ 1798.99.86(a)(2); 1798.140(i).
[17] *See id.*
[18] *See id.* § 1798.99.86(c)(1)(A).
[19] *Id.* § 1798.140(i).

In order to prevent a consumer making a request to delete through the DROP from needing to individually establish their status as a California resident with each registered broker – a version of the **Individualized Consumer Authentication Problem** – the Agency should establish a reasonable procedure for confirming the state residency of a requester before that individual may use the DROP. In addition to solving the **Individualized Consumer Authentication Problem** for state residency, it also protects registered brokers from non-California residents – who have no rights under the CCPA or the Delete Act – from abusing the DROP by submitting fraudulent requests misrepresenting their status as California residents.

The Agency has a range of options for authenticating an individual's state residency before that individual is permitted to use the DROP. At a minimum, the Agency should clearly disclose to individuals seeking to use the DROP that it is available for use only by California residents, and require those individuals to self-report their state residency using a drop-down menu of relevant U.S. jurisdictions.[20] The Agency should prevent any individuals who do not self-report California residency from using the DROP.

However, given the trust that registered brokers would place in the Agency to properly authenticate individuals under Path 2 – as well as the impact of the DROP submitting requests to hundreds of brokers simultaneously – the Agency should take authentication steps beyond self-reporting of state residency. The NAI recommends that the Agency consult with other California authorities that serve California residents to learn about best practices for confirming the state residency of individuals. For example, voter registration in California may involve providing a valid California driver's license number or other California-issued identification card number.[21] While the NAI recognizes that requiring meaningful steps to authenticate state residency beyond self-reporting introduces a degree of friction in the authentication process, the responsibility the Agency would be taking on for authentication under Path 2 demands a higher standard of care to ensure that only California consumers are permitted to use the DROP. Ultimately, the authentication of individuals making requests is an indispensable step that must be completed before registered brokers can verify and act on a VCRs, and the Agency is better suited to perform this rigor more efficiently than each registered data broker doing so independently.[22]

---

[20] Using a drop-down menu instead of a checkbox to report California residency reduces the chance that non-California residents will inadvertently mis-report their state residency by "clicking through" the checkbox.

[21] *See, e.g.,* California Secretary of State, *Voter Registration Application*, Voter Registration Search, https://covr.sos.ca.gov/ (last visited June 25, 2024).

[22] The increased efficiency the Agency could realize from central authentication also supports the symmetry of choice principle found in the CCPA regulations. *Cf.* CAL. CODE REGS., tit. 11, § 7004(a)(2) ("The path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because that would impair or interfere with the consumer's ability to make a choice.").

b. The Agency should not enable consumers to submit identifiers through the DROP that it cannot establish a reasonable authentication procedure for; and should establish reasonable authentication procedures for each identifier the DROP will support.

One of the key benefits of Path 2 is preventing the **Individualized Consumer Authentication Problem**. This problem may arise not only with regard to an individual's state residency – discussed above – but also with regard to the identifiers a consumer wishes to use to effectuate their deletion request. As such, the NAI recommends that the Agency define the specific types of identifiers that may be submitted by consumers using the DROP; and implement reasonable, transparent authentication procedures for each type of allowed identifier. It should do so by enabling consumers to submit only predefined types of identifiers using structured fields. Implementing the DROP in this way also has the benefit of promoting uniformity and administrability of the authentication processes conducted by the Agency, and of implementing the DROP in a more privacy-protecting way.[23]

Without a predefined set of identifiers that the DROP will support, the Agency could find itself seeking to authenticate types of identifiers it has not established policies and procedures for; handling identifiers it cannot reasonably authenticate; or processing more information than is necessary to authenticate an identifier being submitted with the request.

For example, the DROP likely *should* support submission of email addresses and phone numbers because they are commonly used unique identifiers that have reasonable and transparent methods for authentication (*e.g.*, responding appropriately to an authentication message sent to the email address or phone number submitted, which establishes control over the identifier).

However, it is less clear that the Agency should support social security numbers (SSNs) through the DROP if it cannot establish a reasonable and transparent method for authenticating that the individual submitting the SSN is the owner of it. Further, if the Agency determines not to support SSNs through the DROP, this also illustrates why only allowing structured entry of identifiers is called for – the alternative of allowing free-form data entry by requestors could result in the Agency handling data types (like SSN) it may not have adequate security in place for, and that would not facilitate authentication. This approach would also run up against privacy-by-design and data minimization principles by enabling the Agency (and by extension,

[23] *See also* section II.B *infra* for further discussion of how using predefined and structured fields promotes privacy for consumers using the DROP.

registered brokers) to process more personal information than necessary for the purpose of the processing.

c. The Agency should not make a consumer identifier available to registered brokers through the DROP unless all of the Agency's authentication procedures are satisfied.

Building upon the two recommendations above, the NAI also recommends that the Agency only makes an individual's request to delete available to registered brokers to act on through the DROP if: (1) the Agency is able to establish that the requestor is a "consumer"; and (2), if the requestor is a consumer, only those identifiers that the consumer can authenticate with the agency should be made available as part of VCRs sent through the DROP.

The first item reflects the fact that registered brokers are only required to honor deletion requests from consumers; so it would be inefficient and present no benefits to Californians if the Agency included requests from individuals in the DROP that failed to authenticate their California residency.

The second item addresses a distinction between requiring authentication at the consumer level and requiring it at the identifier level – both are necessary to avoid the **Individualized Consumer Authentication Problem.** If authentication occurred at the consumer level only, the Agency might be able to establish, for example, that an individual seeking to use the DROP is named "Jane Doe" and establish that she is a California consumer if she also submits her California driver's license number that matches her name. However, the Agency should not allow this consumer to submit unauthenticated identifiers that she cannot establish control over, because they may not relate to her as a consumer.

Without identifier-level authentication, Jane Doe – even if authenticated as a California consumer – could submit numerous email addresses like 'janedoe1@[].com', 'jane.doe@[].com' and 'jane_doe_14'@[].com' to the DROP even if she did not own or control all (or any) of those email addresses. Registered brokers would also be aware of this and would need to trigger hundreds of authentication emails for all of those email addresses. To prevent this, the Agency should only make identifiers available to be accessed by registered brokers through the DROP if the Agency has already authenticated those identifiers. As with the NAI's other recommendations above, requiring authentication both at the consumer and identifier level helps solve the **Individualized Consumer Authentication Problem** and helps protect brokers from needing to process inauthentic or fraudulent requests.

d. Special considerations for pseudonymous identifiers.

NAI member companies are in some cases distinctive among other types of data brokers because they may process only pseudonymous identifiers like device or cookie IDs that consumers cannot as readily access, provide, or authenticate in the same way that they may be able to do for personal identifiers like email address or phone number. These types of identifiers require different types of authentication procedures, depending on the specific type of pseudonymous ID. In 2019, the NAI issued detailed analysis and guidance related to verification of consumer requests for advertising technologies in response to the CCPA's passage.[24] Much of this guidance is still applicable and the NAI recommends referring to it as a resource for general considerations for verifying consumer requests using technology and with pseudonymous identifiers. Beyond those general considerations, we are also providing several examples with specific considerations for authentication below.

Mobile Advertising IDs

The Agency should consider how it would authenticate mobile advertising IDs (or "MAIDs," such as for Apple iOS[25] or Google Android[26] operating systems). In some cases consumers can access MAID through their device settings; but in other cases MAID can only be accessed programmatically by apps installed on the device. Further, even if MAID is user-readable from device settings, allowing consumers to submit a MAID through the DROP without authenticating it in some way would likely lead to the **Individualized Consumer Authentication Problem** in this context as well. To address this problem, the NAI recommends that the Agency develops a mobile application in connection with the DROP that would enable the Agency to read an authenticated consumer's MAID for the device on which they have installed the app. Installing and running the app demonstrates a degree of control over the device and associated MAID that the NAI believes meets or exceeds common industry practices with respect to authentication of MAIDs; and, as discussed above, if the Agency will take on the responsibility of authenticating identifiers for requests that will be relied on by hundreds of registered brokers, it should take a reasonable, but robust approach to authentication.

---

[24] *See* Network Advertising Initiative, *Analysis of Verifiable Consumer Requests* (2019), https://thenai.org/wp-content/uploads/2021/07/naianalysis_verifiableconsumerrequests9_2019.pdf (last visited June 25, 2024).

[25] *See* advertisingIdentifier, Apple Developer, https://developer.apple.com/documentation/adsupport/asidentifiermanager/advertisingidentifier (last visited June 25, 2024).

[26] *See* Google Support, *Advertising ID*, Play Console Help, https://support.google.com/googleplay/android-developer/answer/6048248?hl=en#:~:text=The%20advertising%20ID%20is%20a,reset%20or%20delete%20their%20identifier (last visited June 25, 2024).

Cookie IDs

The Agency should also consider how it would authenticate business-specific or proprietary identifiers like cookie IDs. The NAI has experience with processing consumer requests for this type of ID for purposes of communicating consumer requests to opt out of interest-based advertising to participating NAI member companies. To communicate this type of consumer request, the NAI relies on an online service at optout.networkadvertising.org that makes a network call to specific endpoints set by each participating NAI member company, enabling them to directly read third-party cookies (3PC) and IDs contained therein for purposes of processing opt-out requests. If the Agency intends to support cookie IDs through the DROP, the NAI would recommend building a similar online service that would call an endpoint for each registered broker that uses 3PC to enable them to directly read cookie IDs for authenticated consumers. Without a central authentication method like this, consumers would have to inspect individual cookies on their browser and enter any IDs contained therein into the DROP interface. In addition to being extremely burdensome for consumers, this would also raise separate authentication issues.

The NAI is also mindful, however, that support for 3PC by major web browsers is declining. Certain web browsers already deploy some level of "tracking" prevention or otherwise limit the use of 3PC by default.[27] Further, if Chrome is allowed to follow its publicly announced timeline, it will no longer support 3PC by mid 2025.[28] The anticipated result is that approximately 97% of web users will experience limited or no functionality for 3PC by default before the DROP is required to be deployed by the Agency in 2026.[29] Beyond that, California consumers already have a powerful method in Global Privacy Control (GPC) implementations for submitting requests to opt out under the CCPA in the web browser environment.[30] While it does not specifically support deletion requests, the NAI believes GPC provides a meaningful option for consumers to limit processing of personal information about them through 3PC at scale. As such, the NAI questions whether designing the DROP to support authentication and

[27] *See, e.g.,* John Wilander, *Intelligent Tracking Prevention*, WebKit Blog (June 5, 2017), https://webkit.org/blog/7675/intelligent-tracking-prevention/ (last visited June 25, 2024); *see also* Mozilla Support, *Enhanced Tracking Protection in Firefox for Desktop*, Firefox Desktop https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop (last updated Mar. 4, 2024); *see also* Microsoft, *Tracking Prevention in Microsoft Edge*, Microsoft Edge Web Platform Documentation (June 19, 2023), https://learn.microsoft.com/en-us/microsoft-edge/web-platform/tracking-prevention (last visited June 25, 2024).
[28] *See* Google Privacy Sandbox, *Prepare for Third-Party Cookie Restrictions*, Google Developers, https://developers.google.com/privacy-sandbox/3pcd (last visited June 25, 2024).
[29] *See United States Browsers Market Share*, SimilarWeb, https://www.similarweb.com/browsers/united-states/ (last visited June 25, 2024).
[30] *See* Global Privacy Control, https://globalprivacycontrol.org/ (last visited June 25, 2024).

transmission of identifiers stored in 3PC will have any material benefit for consumers that would outweigh the costs to the Agency for building a proper authentication method for them.

Hashed identifiers

Some companies process tokenized information about consumers for purposes of digital advertising that is derived from a consumer-provided identifier like an email address or phone number. Consumer-provided IDs may then be hashed, salted and/or encrypted using standard or proprietary methods. The Agency should consider whether it will apply certain standard hashes (like MD5 or SHA256) to authenticated IDs like email address or phone number and make those available to registered brokers through the DROP.

> *4. If following Path 2, the Agency should develop a uniform way for registered brokers to object to the Agency's determination that an individual (or an identifier) is properly authenticated.*

Although the NAI believes unequivocally that the Agency should authenticate requests to delete made through the DROP to avoid the **Individualized Consumer Authentication Problem**, any authentication procedures adopted by the Agency will likely be imperfect. As such, in circumstances where a registered broker has reason to believe that a request received through the DROP was incorrectly authenticated, the Agency should include in the DROP a way for the registered broker to object to the request.

For example, if the Agency authenticates that an individual using the DROP is a California resident, but a registered broker receiving that individual's deletion request through the DROP has specific information indicating that the individual is not a California resident (*e.g.*, because of information indicating current residency in a different state), that broker should be able to object to processing the request sent through the DROP. Note, that under the distinction between authentication and verification, objecting to *authentication* would mean that the registered broker would not be required to process the request as *unverified* (resulting in opting the individual out); but rather would assert that the individual making the request is not entitled to do so, either in general or with respect to a specific identifier.

In turn, the Agency would need to develop a procedure for addressing and resolving objections from registered brokers, either confirming the Agency's authentication of the individual or withdrawing it. If the Agency developed robust authentication procedures as recommended in Section I.B.3 above, this type of objection would likely be rare; further, to the extent an objection is raised, the outcomes would only be positive. If a broker had inaccurate information

about, *e.g.* state residency, then updating it would result in more easily honoring a California consumer's rights; and if the Agency misclassified an individual as a California resident, then the objection would prevent an individual who is not a "consumer" from misusing the DROP.

II. Privacy-protecting

A. Agency Prompt:

"The Delete Act requires the Agency to determine "one or more privacy-protecting ways" by which a consumer can securely submit information to aid in a deletion request using the accessible deletion mechanism. a. How should a consumer securely submit information in a "privacy-protecting way?" b. In what privacy-protecting ways can data brokers determine whether an individual has submitted a deletion request to the Agency?"[31]

B. NAI Responses:

The agency should prioritize using "privacy protecting ways" to design the DROP considering both: (1) how consumers will submit information to the Agency to aid in deletion requests; and (2) how data brokers will access that information to process those requests..

First, to minimize the amount of personal information it collects from consumers, the Agency should not enable consumers to submit free-form or superfluous personal information that is not anticipated to facilitate the Agency's ability to authenticate the individual. Neither should the Agency enable consumers to submit identifiers that are not supported by the DROP. Instead, the Agency should only collect identifiers in connection with a consumer's deletion request if the DROP supports those types of identifiers and includes reasonable authentication procedures for them.[32] To further minimize data collected by the Agency and registered brokers for purposes of verifying requests, the data elements should be structured and should not support free-form entry, which further defines and minimizes that types of personal information the Agency will collect only to what is necessary to process the request.

Second, in facilitating data broker access to consumer requests to delete, the DROP should rely on a secure, programmatic method for registered brokers to look up identifiers that the Agency has authenticated. This could, for example, be a secure API that allows registered brokers to look up only those identifiers it actually processes in its data product(s) and that the DROP supports. The DROP should also prevent a broker from accessing a type of identifier that the broker does not process in its data product(s) in order to prevent that broker from even

[31] *See* Request for Comments, *supra* note 1.
[32] *See also* Section I.B.3.b *supra* for further discussion of this point.

accidentally matching its existing identifiers with new personal information made available through the DROP.[33] In other words, the DROP should be designed to prevent brokers from learning anything new about a consumer making a request, and should only make available information the broker could actually use to match and act upon an authenticated request made through the DROP.

III. Status of Request

A. Agency Prompt:

"The Delete Act requires the accessible deletion mechanism to allow the consumer, or their authorized agent, "to verify the status of the consumer's deletion request." a. What information should be included in the "status of the consumer's deletion request"? b. For consumers, what are your preferred ways to verify the status of your request? (i.e., settings within the deletion mechanism, email, platform interface, etc.)? c. For businesses, do you currently allow consumers to verify the status of their CCPA privacy requests? How so? What are your preferred ways to allow consumers to verify the status of their CCPA privacy requests? Why?"[34]

B. NAI responses:

The information included in the "status" of a consumer's request presented through the DROP should be simple and easy to understand for consumers, track registered brokers' legal obligations in processing properly submitted VCRs, and be implemented programmatically to improve efficiency for the Agency and registered data brokers.

The Delete Act requires registered brokers to access the DROP at least once every 45 days, and act on deletion requests accessed through the drop within 45 days after receiving them.[35] Because registered brokers are only required to access the DROP once every 45 days, it follows that there will in many cases be a delay between the time a consumer submits a request through the DROP and the time a registered broker accesses that request. Further, different registered brokers may access the DROP at different times. As such, the NAI recommends that a status tracker for the DROP be capable of informing a consumer that has made a request that her request, *for each separate broker*, is:

---

[33] *See* CAL. CIV. CODE § 1798.99.86(b)(3) (specifying that the DROP should "not allow the disclosure of any additional personal information" to brokers beyond what is necessary to determine whether the consumer has submitted a VCR).
[34] *See* Request for Comments, *supra* note 1.
[35] CAL. CIV. CODE § 1798.99.86(c)(1)(a).

- "Pending" for a broker if it has been successfully authenticated by the Agency and made available to registered brokers, but not yet accessed by the particular broker;
- "Received" for a broker if that particular broker has accessed the deletion request (which would also trigger the 45-day period a broker is allowed to complete its processing of the request);
- "Withdrawn" for a broker if the consumer that has previously requested deletion changes her election through the DROP for a particular broker; or
- "N/A" or other similar messaging if the consumer never elected to request deletion from a particular broker.[36]

The Agency may also consider whether additional and more granular statuses are appropriate for the DROP; however additional statuses would likely lead to greatly increased complexity and administrative costs for both the Agency and registered brokers. For example, the DROP could also include statuses for the disposition of a consumer's request, such as:

- "Completed – Personal Information Deleted" if the broker is able to verify and act on an authenticated consumer request to delete received through the DROP;
- "Completed – Opted Out" if the broker is unable to verify (*i.e.*, match) a consumer request that was properly authenticated by the Agency through the DROP, but opts that consumer out as required by the Delete Act; or
- "Objection" if the broker objects, *e.g.*, to the Agency's authentication of the individual as California "consumer."[37]

However, including additional status information such as the examples above would require the DROP and registered brokers interfacing with it to process multiple additional data points in a uniform way that will necessarily increase the complexity of the system. The additional status options may also prove confusing to consumers. Therefore, the NAI recommends that the Agency use only the simpler, clearer, and easier-to-implement statuses above.

IV. Consumer Experience

A. Agency Prompt:

"The Delete Act requires the accessible deletion mechanism to allow a consumer, "through a single verifiable consumer request," to request that every data broker that any personal

[36] *See id*. § 1798.99.86(a)(3) (requiring the DROP to support selective inclusion/exclusion of specific brokers).
[37] *See* § I.B.4 *supra* for more discussion of the NAI's recommendation that the DROP supports a way for brokers to issue such objections.

information [sic] delete any personal information related to that data broker or associated service provider or contractor. a. What should the Agency consider with respect to the consumer experience? b. How can the Agency ensure that every Californian can easily exercise their right to delete and right to opt-out of sale and sharing of their personal information via the accessible deletion mechanism?"[38]

B. NAI responses:

Consumers using the DROP should be presented with fair, complete, and accurate disclosures and descriptions about the type of request they are able to make using the DROP. For consumers to make an informed choice, this should also include information about the potential drawbacks of deletion by all registered brokers. For example, effectuating a deletion request may hamper the ability of registered brokers to match the consumer to products and services they may be interested in through advertising and marketing.

Further, because of the consequential nature of submitting a deletion request simultaneously to all registered brokers, the Agency should include second-layer confirmation of the request; and consumers making such requests through the DROP should be notified that a successfully processed deletion cannot be undone.

Finally, because a consumer may decide to withdraw a deletion request (*e.g.*, if the consumer does not want some or all registered brokers to continuously delete their personal information but instead wants to "reset" a broker by requesting deletion once), the DROP should make it as easy to withdraw a request to delete as to make one.[39] This would be consistent with the Agency's guidance on choice architecture in other arenas and for avoiding dark patterns.[40]

V. Additional Comments

A. Agency Prompt:

"Please provide any additional comments you may have in relation to the accessible deletion mechanism."[41]

[38] *See* Request for Comments, *supra* note 1.
[39] *See* Cal. Civ. Code § 1798.99.86(a)(4).
[40] *See, e.g.,* Cal. Code Regs., tit. 11, § 7004(a)(4).
[41] *See* Request for Comments, *supra* note 1.

B. NAI Responses:

The Agency should carefully consider how it will confirm that an authorized agent seeking to make a VCR on behalf of an individual meets the applicable legal requirements for doing so (*i.e.*, is registered with the secretary of state)[42] and has the actual authority to act on behalf of the individual.

Further, it is imperative that the Agency distinguish between determining whether an authorized agent is eligible to assist an individual in making a *request* through the DROP[43] and whether the Agency has authenticated the individual whom the authorized agent is acting on behalf of. Some consumers might find it helpful to use an authorized agent to submit requests on their behalf – both to data brokers and to other California businesses – but the Agency must not cede the task of authenticating those individuals to authorized agents. This is because neither the Agency nor registered brokers would have any transparency into how – or even whether – the authorized agent has properly determined that they are submitting a request on behalf of an individual entitled to make that request or whether any identifiers being submitted actually relate to the individual the authorized agent purports to be representing. The risk of the DROP being abused without robust authentication by the Agency – especially for requests made by authorized agents – is too high and will likely lead to the **Individualized Consumer Authentication Problem** arising in this context if registered brokers do not have transparent authentication processes to rely on for authorized agent requests.

To avoid complications around authorized agent requests, the NAI recommends that the Agency take the following steps:

- Require individuals initiating a request through the DROP to specify whether they are making the request on their own behalf or on behalf of another individual as an authorized agent;
- For individuals identifying their request as being made as an authorized agent, the Agency should cross-reference the identity of the requesting authorized agent service with registrations maintained by the secretary of state to confirm they meet the CCPA requirements for registration;[44] and
- Require reasonable proof that the individual making a request as an authorized agent has actual authority to act on behalf of the other individual, such as by requiring

[42] *See* CAL. CIV. CODE § 1798.140(ak) (specifying that an authorized agent submitting a VCR on behalf of a consumer must be registered with the secretary of state).
[43] *See id.* § 1798.99.86(b)(8) (specifying that authorized agents should be able to aid in consumer's deletion *request*).
[44] *See id*.

presentation to the Agency and manual review of an authorization signed by the individual.

If an authorized agent meets these requirements, the Agency should then initiate its authentication procedures directly with the individual being represented using the identifier(s) provided by the authorized agent – for example, by sending confirmation communications and taking other steps discussed in more detail above in section I.B.3 of these comments.

Finally, the Agency should include in the information made available to registered brokers through the DROP an indication that the request was initiated by an authorized agent and not by the consumer directly.

VI. Conclusion

The NAI appreciates the opportunity to submit comments to the Agency on these important topics. If we can provide any additional information, or otherwise assist your office as it continues to engage in the rulemaking process, please do not hesitate to contact me at tony@networkadvertising.org, or David LeDuc, Vice President, Public Policy, at david@networkadvertising.org.

*****

Respectfully Submitted,

Tony Ficarrotta
Vice President & General Counsel
Network Advertising Initiative (NAI)