From: Brian May
To: DataBrokers@CPPA
Subject: Preliminary Comment DROP 06-24
Date: Tuesday, June 25, 2024 1:30:10 PM

Resubmitting after seeing the requested subject line in the response to my original submission.

On Tue, Jun 25, 2024 at 4:27 PM Brian May [redacted] wrote:

> I have some general thoughts followed by answers to specific questions in the INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING UNDER SENATE BILL 362.
>
> What identifiers are subject to deletion requests? In order to request deletion, there must be a means of identifying what data is to be deleted and there needs to be some means of demonstrating ownership of said identifier. If the deletion requirement is limited to deterministic data related to specific, persistent identifiers like email address and phone number, then executing them is relatively straightforward. If, on the other hand, the requirement encompasses data associated with a cookie ID, an IP address, a probabilistic ID or other identifiers that are not directly available to users or under their control, identifying identifiers, verifying ownership and communicating them becomes a much harder set of problems to solve.
>
> How is the requirement that there be a single request reconciled with the fact that folks have multiple forms of ID – a phone number, generally at least a couple of email addresses and others? Is the intent for the user to create a deletion request profile and add to it each form of ID they believe is, or might be, used by data brokers? If so, what of the threat posed by maintaining a database containing comprehensive lists created by users of the identifiers associated with them? A breach of such a database would represent a significant privacy threat.
>
> Does the requirement that there be a single request imply that data brokers will be provided with sets of identifiers for requesters and thereby a source of information for building out identify graphs or is there an intent to convert a single request by a user containing multiple IDs into atomic, individually processed, per-identifier transactions?

Post deletion verification at scale could be challenging. A potential means of auditing compliance would be to require data brokers to provide auditors with access to the same APIs used by their partners so auditors could call them with an identifier deletion had been requested for and verify that what the API returned did in fact indicate the data was not available. Auditors could check on a small, random sample of identifiers continuously across all brokers as a way of monitoring compliance.

Proof of ownership – with email and phone number it is relatively straightforward, send a code and have the recipient enter it. With other forms of identification it is much less clear how to provide proof of ownership without also providing additional personal information.

Are data brokers required to delete all data associated with an identifier, including any other identifiers? If so, is there any requirement that brokers indicate what identifiers they maintained in association with the identifier subject to the deletion request? If not, how are brokers prevented from deleting just an identifier associated with a user profile and continuing to maintain the profile in connection with other identifiers? If a broker has a profile of me that includes my phone number and email address and I submit a deletion request for the phone number, is the data broker required to assume the email address is also an identifier that is covered by the request or can the broker simply delete the phone number from the profile?

Is there a requirement that data brokers who have shared data with partners, and subsequently receive a deletion request for the shared data, provide information about what partners the data has been shared with? If not, how does the user determine if a request is complete and comprehensive?

Answers to some specific questions from the invitation:

1.a. What should constitute a "verifiable consumer request"?
I think the same measures applied when a consumer creates a new account could be applied to deletion requests. For requests based on an email address or phone number, send a message from the deletion registry that includes a code which the recipient provides to prove they have access to the email account or phone number deletion is being requested for. It should be the Delete Requests and Opt-Out Platform that does the verification and all requests communicated to data brokers should be assumed to be verified.

2.a. How should a consumer securely submit information in a “privacy-protecting way?”
I think the best way to assure consumer privacy is protected is to use mechanisms similar to those used for protecting account authentication credentials:

- All interactions happen in a secure context.

Any information which can be maintained in hashed form, should be. For example, a submitted email address could be hashed in a standard way and the hash provided to data brokers rather than the original email address. Brokers on their side would maintain a hashed version of all email addresses which they could use to look up data to be deleted.

- Any information that can't be maintained in hashed form should be encrypted.

2.b. In what privacy-protecting ways can data brokers determine whether an individual has submitted a deletion request to the Agency?
Per the second bullet above, identifiers can be hashed by the DROP upon verification. The hashes can then be provided to data brokers in a set of lookup tables grouped by request period (e.g. monthly) which are available for download from the DROP. On their side, data brokers could maintain versions of all their identifiers hashed using the same method as the DROP platform and then join their tables to the data in the DROP lists to identify profiles for which deletions were requested. This allows brokers to identify data that should be deleted for any identifier they have previously encountered without exposing to them identifiers they have not previously encountered.

3.a. What information should be included in the “status of the consumer’s deletion request”?
When a request was received, it should be recorded as having been received by the broker even if the broker doesn't have data associated with the identifier that is the subject of the request. If data is subsequently shared with the broker, it should immediately be deleted. If data has been queued for deletion, the status should be "pending". If data is being deleted status should be "in progress". If data has been deleted, status should be executed and the result of the execution. The latter should usually be "data deleted", but there may be other outcomes that would be of interest to consumers, for example if the broker was not able to delete the data for some reason.
3.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.)?
In order to protect the privacy of consumers, the DROP should act as intermediary gathering deletion statuses so that consumer information isn't directly exposed to brokers. The more passive the means by which the DROP gathers the data, the better. So, ideally brokers would be required to provide status information for requests to the DROP which would update consumer accounts accordingly and allow consumers to learn the status of their requests without broker interaction.

4.a. What should the Agency consider with respect to the consumer experience?
It is very common for consumer information to be distributed to many parties the consumer has never interacted with directly and so wouldn't know to make a deletion request to. It would be very helpful to provide consumers with information about all brokers that received their deletion request and all partners they forwarded it on to, along with an indication of the status of the request for each entity. This would allow consumers to understand with whom their data had been shared and what its status was.
4.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?
Allow requests to be made via: an online request form, email, text or phone call. One area of concern is providing consumers with information about what identifiers are used to gather data related to them. This may be the DROP to request from brokers the list of alternate identifiers they have associated with a specific consumer identifier so that the consumer can

> gather a comprehensive list.
>
> --

Brian May

Principal Engineer

[redacted]

[redacted]

--

Brian May

Principal Engineer

[redacted] [redacted]

experian.

[redacted]

June 25, 2024

Via electronic filing

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

Re: Preliminary Comment DROP 06-24

California Privacy Protection Agency Board:

On behalf of Experian, we submit these comments in response to the California Privacy Protection Agency's ("CPPA" or "Agency") invitation for preliminary comments on the proposed rulemaking under Senate Bill 362 (the "Delete Act").[1] Respecting consumer privacy is central to Experian's corporate principles and operational values. Consumer trust and effective stewardship of information are vital to our company's continued success.

As described in more detail below, Experian's products and services provide significant benefits to consumers and businesses. For example, our offerings provide value by, among other matters: protecting families from identity theft and fraud; enabling small businesses to find customers for their offerings; informing consumers about products and services that are relevant to them; and helping to notify consumers of new vehicle safety recalls. All of these offerings rely on data to function. As the Agency considers regulations to implement the Delete Act and stand up the Data Broker Delete Requests and Opt-Out Platform ("DROP"), we ask the CPPA to carefully consider how its regulations could impact the ability of Californians and California businesses to reap the benefits of these useful services and services like them in the marketplace.

Our comments first provide an overview of Experian's offerings to demonstrate the benefits consumers derive from our products and services. We next ask the Agency to clarify to consumers the scope and limit of actions made via DROP; in particular, we ask the CPPA to clarify that requests through the DROP will not be applied in cases where when personal information will be used for security and integrity purposes. Next, we offer targeted input on parameters the Agency should set for validating agents' authority to act on behalf of consumers and for verifying consumer requests. We offer these comments with the goal of enhancing consumers' privacy while ensuring consumers' rights are effectively carried out in accordance with their expectations.

[1] California Privacy Protection Agency, *Invitation for Preliminary Comments on Proposed Rulemaking Under Senate Bill 362* (May 31, 2024), located here.

I. Experian provides various beneficial products and services to the marketplace that improve consumers' lives.

Experian is made up of several business units that process data to provide products and services that benefit consumers and enrich their lives. In addition to our core consumer reporting agency services, which are regulated under the Fair Credit Reporting Act ("FCRA") and are outside of the scope of the Delete Act, Experian provides a wide variety of offerings that bring value to consumers directly or indirectly.

We provide, for example, vehicle history and recall notice services that allow consumers to be contacted with crucially important information about recalls that may impact their safety. We also provide fraud prevention and identity resolution services that keep consumers safe when transacting in the marketplace. We provide data quality and validation services that allow organizations to improve data accuracy and authenticate and validate consumer contact information. These are just a handful of examples of the important and valuable products and services Experian provides to the benefit of consumers. Each of these services is reliant on data; without the data needed to bring these offerings to the market, consumers will be less safe, harder to reach, and will have fewer choices of businesses to frequent and patronize.

In addition, under the larger Experian umbrella is Experian Marketing Services ("EMS"). EMS helps organizations better understand potential preferences of customers and prospective customers. Users of EMS represent the most trusted brands in nearly every industry, including financial services, media, automotive, travel and leisure, healthcare, retail, government, and non-profits, and they use EMS to create a more relevant experience for customers and prospective customers. EMS is not a "look up" service for organizations or individuals to search for specific consumers, but rather helps further cost-efficient marketing by identifying groups, or audiences of customers, that may have similar interests or preferences. Although marketing techniques have evolved over time, this is the same goal that has driven marketing efforts since well before the present online era.

Consumers benefit directly from data-driven marketing services like those provided through EMS, including through the access they gain to the low-or-no-cost online content that often flows from advertising. For many types of online content, advertising is the primary source of revenue, and it has funded the expansion of the free Internet, including news, blogs, maps, and gaming, as an alternative to the subscription model. It is also a key factor in the innovation and diversity of online services enjoyed by consumers by reducing barriers to entry. Studies have found that limiting access to data about audience interests and demographics reduces revenue for online content providers by 50 to 70 percent, and revenue losses can threaten the financial foundation of free services that have been estimated to be worth $30,000 per year to the typical consumer.[2] In 2021, online advertising represented 64% of total advertising in the United States.[3] Because of responsible data sharing, companies can reach the groups of consumers who are most likely to need and enjoy their offerings. This puts more information in the hands of consumers, helps small businesses grow, increases the availability of nonprofit services for consumers, and promotes competition, which ultimately provides more services and drives down prices for all of us.

II. The DROP should clearly describe the scope of rights requests to consumers on the mechanism page so consumers can make informed choices.

The CPPA should ensure that the webpage accompanying the DROP clearly describes the scope of rights available to consumers and the way that the DROP will function. For example, the CPPA should explain to consumers that requests through the DROP do not apply to personal information and/or entities covered by applicable laws set forth in the Delete Act, such as the FCRA, Gramm-Leach Bliley Act, and the Health Insurance Portability and Accountability Act. The webpage accompanying the DROP should also clearly describe other exemptions and relevant limitations under the Delete Act, for instance, that a request made through the DROP will not limit retention and use of personal information for fraud prevention and security and integrity purposes by data brokers. These disclosures to consumers through the webpage accompanying the DROP are critical so consumers are aware of the scope of their rights.

Experian's broad array of services and robust compliance program make Experian a unique type of data broker in the marketplace. Given Experian's role in the economy, our compliance and due diligence infrastructure may be more robust and rigorous than other data brokers registered under California law. Moreover, our offerings, including our important anti-fraud and identity theft protection services, and our position as a trusted brand consumers recognize, may present unique considerations for consumers as they weigh which data brokers to submit deletion requests to through the DROP. The CPPA should consider grouping data brokers into certain categories to aid in consumers' decision-making. For example, data brokers that provide anti-fraud and identity theft prevention services could potentially be grouped into one category. Data brokers who have documented advanced privacy compliance and operational standards, such as customer credentialing, privacy audits, and privacy roles in the organization, could be identified as a separate category of information service providers. Data brokers that solely provide "look-up" services could be grouped into another category. Transparency and choice will help consumers better decide who to effectuate deletion requests against through the DROP.

[2] *See* J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, at ii (Nov. 2022), https://www.privacyforamerica.com/wp-content/uploads/2022/11/Study-221115-Beales-and-Stivers-Information-Economy-Without-Data-Nov22-final.pdf.

[3] *Id.*

III. The DROP must include protections for consumers when working through an authorized agent to ensure agents are acting in accordance with consumers' informed directions and consumers understand their rights.

The Delete Act states that authorized agents must be permitted to "aid" in consumers' deletion requests through the accessible mechanism.[4] However, the law itself provides little detail surrounding the process for validating agents' authority to act on behalf of consumers or other safeguards they should be subject to in order to protect consumer choice and deter anticompetitive interference in the system by agents.

The CPPA should issue rules, consistent with its regulations implementing the California Consumer Privacy Act ("CCPA"), that permit data brokers to ask authorized agents to provide signed proof of their authority to act on behalf of consumers when submitting requests through the DROP *and* allow data brokers to either (1) ask consumers to verify their identities directly with the data brokers themselves or (2) require consumers to directly confirm to data brokers that they provided an agent with authority to submit a request.[5] In addition or alternatively, the CPPA should define clear and robust procedures it will engage in to validate such agents' authority. The Agency should consider engaging in a rulemaking setting out specifications for validating DROP requests facilitated through authorized agents before permitting authorized agents to submit requests on behalf of consumers.

The Agency should also consider the impact of authorized agents that otherwise provide similar services and compete with registered data brokers. These types of agents should be prohibited from using the deletion mechanism. Agents facilitating deletion requests should be required to register with the Agency to allow CPPA oversight and validation the business is not otherwise competing with registered data brokers. Regulations setting important safeguards around authorized agent requests are necessary to protect consumers and integrity of the DROP.

Specifically, authorized agents should be required conspicuously to inform consumers of the scope and effect of their rights requests, as well as applicable limitations on their rights requests pursuant to Delete Act exemptions as discussed in more detail above. In addition, authorized agents should be required to disclose and provide the same choices the CPPA is required to provide when presenting options to consumers. For example, the Delete Act requires the CPPA to provide the ability for consumers to delete data from individual data brokers so long as a holistic option is also available, allow a consumer to alter a previous request, and provide a description of the deletion permitted, the process for submitting a request, and examples of information that may be deleted.[6] Agents should be required to present these same options and disclosures

[4] *Id.* at § 1798.99.86(b)(8).

[5] *See* Cal. Code Regs. tit. 11, 7063.

[6] *Id.* at § 1798.99.86(a)(3), § 1798.99.86(a)(10).

to consumers. If an authorized agent is charging a fee to facilitate a request through the DROP, the agent should be obligated to conspicuously inform a consumer of the ability to make a request through the DROP at no cost or directly with the data broker.

Agents should also be required to explain the DROP in a neutral manner to consumers and should not be permitted to use dark patterns, coercive or manipulative language, or other methods of sensationalizing or downplaying the effects of using or not using the DROP. In addition, agents should be required to obtain informed consent from consumers to act on their behalf, outside of the context of any broad terms of use or other generic policy presented to consumers.[7] Agents should not be permitted to self-certify their authority to act on behalf of consumers without a separate process conducted by the Agency to validate such agents' authority to act.

The CPPA should also take steps to minimize the potential for authorized agent abuse of the DROP system by promulgating regulations describing how an authorized agent must go about acquiring authorization from consumers to act and presenting terms to consumers. The FTC has acknowledged the potential for agents to abuse their role as an intermediary in other contexts, such as the FTC's do-not-call registry, and consequently set limits on agents' authority to act in that sphere.[8] Absent protective rules surrounding validating authorized agents' authority, agents could potentially send reams of "rights requests" to the CPPA through the DROP by copying and pasting information in the Whitepages without obtaining informed consent to act on behalf of consumers. Agents could also assert that assignment of authority to act was gathered through a consumer's acceptance of general terms and conditions. To help ensure consumers provide informed consent for agents to act on their behalf, the CPPA should issue regulations defining how such authority must be validated.

IV. The DROP must include controls to permit data broker verification of consumer deletion requests.

Verifying the identity of consumers who make deletion requests through the DROP is critically important to ensure data brokers are actioning requests against data

[7] The California Consumer Privacy Act defines "consent" as "any freely given, **specific, informed, and unambiguous** indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. **Acceptance of a general or broad terms of use, or similar document,** that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent." *Id.* at § 1798.140(h). This "consent" should be required of agents seeking authority from consumers to submit deletion requests on their behalf through the DROP.

[8] *See* Federal Trade Commission, *Final Amended Rule: Telemarketing Sales Rule*, 68 Fed. Reg. 4580, 4639 (Jan. 29, 2003); Federal Trade Commission, *Q&A: The National Do Not Call Registry*, located here.

associated with the correct consumer. Absent robust and effective verification measures, data brokers will be unable to ensure they are effectuating a deletion request against the appropriate consumer record. Taking action to delete data associated with the wrong consumer could adversely impact the rights and freedoms of other consumers, an outcome explicitly forbidden under California law.[9] In addition, any rules the CPPA promulgates related to verification in the context of the DROP should centralize verification measures within the Agency or the data brokers that will be responsible for executing deletion requests rather than authorized agents, as described in more detail below.

The CPPA should issue a regulation defining a clear standard the Agency will use to verify requests submitted through the DROP. The CPPA should consider implementing verification standards that are consistent with CCPA regulations and are sufficiently robust to protect against fraudulent requests or requests that have been spoofed or fabricated. The Agency should also consider implementing more stringent verification requirements to consider the risk of harm to the consumer posed by unauthorized deletion of personal information. The risk of harm to consumers from unauthorized deletion warrants a high level of assurance that the information deleted from data broker systems aligns with the consumer who initiated the request.

To help ensure requests through the DROP are actioned against the correct consumer record, appropriate verification measures may, in certain instances, require consumers to confirm their identities directly with data brokers rather than through the CPPA or other measures associated with the DROP. Authorized agents should not be permitted to verify consumer requests because each individual data broker's verification process may require different data points to locate and verify a consumer request through its unique systems. The Delete Act defines "data broker" broadly to encompass many kinds of entities in the marketplace.[10] Data brokers may maintain different information about individuals depending on the services they offer, communication channels they support, and the industries they serve. In particular, data brokers may not collect and maintain the same types of data elements, meaning a variety of verifying data points may be necessary to effectuate requests. As a result, verification rules should permit data brokers themselves to independently verify consumer requests and should allow for reasonable flexibility in such data brokers' verification procedures. Different data brokers may need to take different steps to verify given the types and scope of data maintained. Deferring to data brokers' own verification processes consequently may be necessary to ensure consumers are appropriately verified in accordance with law.

*   *   *

[9] *Id.* at § 1798.145(k).
[10] *Id.* at § 1798.99.80(c).

Thank you for your consideration of these comments.

Sincerely,

Liz Oesterle

Elizabeth Oesterle
Senior Vice President, Government Affairs

IN-HOUSE PRIVACY

June 25, 2024

In-House Privacy, Inc. Response to Preliminary Request for Comments by the California Privacy Protection Agency

Introduction: In-House Privacy, Inc. ("IHP") is a California-based boutique law firm and privacy consultancy focused primarily on servicing clients in the advertising and marketing industries, including a number of companies registered as 'data brokers' with the California registry as prescribed by SB 362. The following responses are based on a collection of opinions by the principles at In-House Privacy, Inc. and data broker industry stakeholders. They do not represent or reflect the opinions or positions of any particular In-House Privacy, Inc. client or their employees.

1. Verifiable Consumer Requests

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.[5]

a. What should constitute a "v*erifiable consumer request*"?[6]

IHP Response:

1. **California Residency.** Many individuals who are not California residents regularly attempt to obtain California-specific rights. While many other U.S. states have followed California's lead in enacting similar laws with consumer deletion rights, numerous individuals ignore their residency requirements when submitting data deletion requests. As a result, attempts to verify their residency through the provision of a government-issued identifier or other proof of residency often fail to determine that they are California residents. For example, an IHP client (not a data broker) observed during the first year of CCPA compliance that nearly 65% of all access or deletion requests came from consumers outside of California even though the client created a specific form and self-attestation that the form was to only be used by California residents.

   As a California government agency, it is recommended that the CPPA collaborate with the Department of Motor Vehicles, franchise tax board, or other government agencies to create a streamlined process for California consumers to be easily verified in advance of enabling consumers to utilize the CPPA Deletion Mechanism. This proof of residency requirement should be renewed each year should the consumer wish to continue utilizing the Deletion Mechanism.

2. **Auditable Verification.** Consumers have become accustomed to confirming their email address when they subscribe to email newsletters or updates, and the CPPA should ensure that any consumer utilizing the Deletion Mechanism clicks through an email that they receive from the CPPA in order to confirm their ownership, or authorized use, of the email submitted to the Deletion Mechanism. Should the CPPA enable multiple email addresses by the same consumer, to prevent abuse of the Deletion Mechanism, all such emails must also be confirmed through a similar email-specific confirmation mechanism. Should the CPPA expand to postal addresses or phone numbers, a similar method should be utilized based on uploading a name-specific postal receipt or SMS/call-based verification of phone numbers. The records for these

confirmations should be maintained by the CPPA, and the user should be required to re-verify their contact information annually in order to continue utilizing the Deletion Mechanism.

1.

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?

IHP Response: The complexity and cost of managing consumer privacy rights verification is increasing for data brokers. Most data brokers IHP works with require proof of identity and/or California residency in order to effectuate a deletion request, as opposed to opt out requests which do not require any such verification. In most instances, the consumer is required to upload through a web form a government-issued identification card. While there are some specific software solutions to make this webform easy to use, it still typically requires that the data broker review each identification record for California verification. IHP is unaware of any data brokers currently paying for or otherwise utilizing software or services that would streamline the process of verifying consumer identifies, such as 'Know Your Customer' ('KYC') software provided for banking or financial institutions to comply with anti-money laundering regulations. These KYC software solutions are not offered by 'privacy technology' companies, nor are they cost-effective for data brokers to effectuate for consumer privacy requests. However, if the CPPA collaborated with a KYC software solution and provided it for free to data brokers, it is likely that the data broker industry would cooperate with such a service.

2. Privacy-protecting

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.[7]

a. How should a consumer securely submit information in a "*privacy-protecting way*?"[8]

IHP Response: The best practice for the CPPA to validate consumers in a privacy-protected way would be to utilize a KYC software software solution commonly utilized by the financial services industry to comply with anti-money laundering laws. These tools are proven to accurately identify individuals and their state-specific residency in an easily accessible mechanism.

b. In what privacy-protecting ways can data brokers determine whether an individual has submitted a deletion request to the Agency?

IHP Response: For decades, the direct marketing industry has utilized trusted intermediaries to combine data sets for various purposes including suppression of personal information. Specifically, since the enactment of the CAN-SPAM Act in 2003, email marketers utilizing third party email lists have been required to share suppression lists with the email provider to effectuate opt outs, which has led to the creation of numerous 'suppression automation' services. These trusted intermediaries are paid exclusively for their matching and suppression services, and do not otherwise utilize the data for any other derivative purposes. The CPPA could contract with one of these types of intermediaries to provide this automation service on data brokers behalf rather than create a new database run by a governmental organization.

In recent years, the advertising industry has been utilizing software that synchronizes personal information between disparate parties without the personal information ever being accessible by the other party. This ‘data clean room’ software also utilizes privacy-preserving methods to obfuscate the personal information so it is limited to exact data matches. The CPPA could explore some similar software to enable synchronization of information without ‘sharing’ the personal information. The end result would be that the data brokers could receive a ‘net suppression’ list of their personal information on a regular basis, without any need to access or otherwise derive the identities of the individuals requesting deletion. For data brokers, there is no real need to ‘determine a submission’, as the effect of removing the verified consumer in an efficient manner is sufficient to comply with the law. As long as the CPPA, intermediary or software solution records the information in a way that validates the effect to the data broker through an auditable, automated feedback loop, then this should be sufficient.

3. *Status of Request*

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.”[9]

a. What information should be included in the “*status of the consumer’s deletion request*”?[10]

IHP Response: There are two pieces of information to be included in such a status update;

1. The status of the consumer's verification of the contact information provided, such as the date and time of their email confirmation and the date in which it must be reconfirmed in order to be retained.
2. With the delete mechanism, there are varying levels of transparency possibilities, ranging from the basic ‘date in which information was made available’ to data brokers, to ‘confirmation that data brokers have begun processing the data’, to ‘confirmation that all registered data brokers have processed the data’, but more specifically it could be sophisticated enough to identify each registered broker and their accessibility status on a monthly or other regular basis. If the CPPA were to use software such as those used by intermediaries or data clean rooms, there could be more detailed information provided on the date, time and access success associated with each deletion record. Such status markers have been productized to various degree by popular consumer 'delete me' apps and services, and the CPPA could help standardize the details provided.

[4] Civil Code, § 1798.99.87(a)
[5] Civil Code, § 1798.99.86(a)(2)
[6] Civil Code, § 1798.99.86(a)(2)
[7] Civil Code, § 1798.99.86(b)(2)
[8] Civil Code, § 1798.99.86(b)(2)
[9] Civil Code, § 1798.99.86(b)(9)
[10] Civil Code, § 1798.99.86(b)(9)

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?

1. Many data brokers send an email to the requesting consumer notifying them that their deletion request has been processed in a ‘batch’ with other deletion requests on a monthly basis or other regular cadence, or more often that the request ‘will be processed in the next [X] days’.

   However, IHP is unfamiliar with any data brokers that enable a ‘verification’ of the status of the deletion request. If the data broker has deleted the information, then it seems contradictory to ‘verify’ such a status. However, as long as the CPPA, intermediary or software solution records the action of the data broker, consumers should be able to check the status of their verified request through that solution, using a unique request number or similar case-identifier.

4. *Consumer Experience*

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 information delete any personal information related to that data broker or associated service provider or contractor.[11]

a. What should the Agency consider with respect to the consumer experience?

IHP Response: The key issue for the CPPA is to mitigate against abuse of the Deletion Mechanism by unscrupulous actors. When the Federal Trade Commission created the ‘Do Not Call’ registry, there were many reports of attempted abuse of erroneous information being submitted through various automated means. The CPPA will have an important task to mitigate any such abuse by confirming all contact information, using automation filtering tools such as CAPTCHA, throttling the number of requests a particular browser or device can submit in short succession, utilizing external software to avoid bots or scripts being utilized on the site, and ideally using a ‘Know Your Customer’ authentication tool to validate California residency to minimize friction with other verification approaches.

5. *Additional Comments*

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

IHP Response 1: The CPPA does not include any requests for preliminary comments with respect to the use of Authorized Agents to utilize the Deletion Mechanism on behalf of their California resident customers. It is recommended that the CPPA include the potential for these services to be used, and whether their customers are ‘verified California residents’ through similar mechanisms in which the CPPA may implement on its own. In addition, the CPPA may consider the use of automated programming interfaces (API) to facilitate direct interactions with authorized agents, as well as data brokers, to effectuate deletion requests. While the goal of any such effort is clearly efficiency, the CPPA will also have a responsibility to ensure that any such authorized agents do not abuse any such automation approaches and are either ‘certified’ by the CPPA to use any such automation, and/or are regularly audited by inside or outside auditors to ensure their systems are in compliance with any such CPPA regulations.

IHP Response 2: It is recommended for the CPPA to conduct a survey of data brokers on the anticipated costs for compliance with the Delete Mechanism, and report to the public on the average anticipated costs to comply. This survey should take place following the final specifications for the Deletion Mechanism, and steps required of data brokers to comply. These costs will include development time, software utilized, processing compute costs, hosting or cloud software fees, employee maintenance, auditing, legal and/or compliance support, and other costs.

June 25, 2024

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

RE: Preliminary Comment DROP 06-24 – Joint Ad Trade Letter: Initial Comments on Proposed Rulemaking under Senate Bill 362 (California Delete Act)

Dear California Privacy Protection Agency:

On behalf of the advertising industry, we provide these comments in response to the California Privacy Protection Agency's ("CPPA") request for preliminary comment ("RFC") on the proposed rulemaking under Senate Bill 362 ("California Delete Act").[1] We and the companies we represent, many of whom do substantial business in California, strongly believe consumers deserve meaningful privacy protections supported by reasonable laws and responsible industry policies. We provide these initial, non-exhaustive comments with the goal of informing the CPPA of potential unforeseen consequences the California Delete Act regulations could create and advocating for strong yet flexible rules to help ensure Californians' choices are accurately carried out and data brokers are functionally able to process deletion requests made through the Data Broker Delete Requests and Opt-Out Platform ("DROP"). We thank you for the opportunity to participate in this regulatory process.

Below we provide comments on five discrete areas the CPPA should consider as it develops draft rules: (1) validating the authority of authorized agents to act on behalf of consumers; (2) establishing important safeguards for requests submitted through authorized agents; (3) consumer verification processes for requests submitted through the DROP; (4) clarifying the California Delete Act's applicability to data used to provide critical anti-fraud products and services; and (5) the CPPA's potential changes to the definition of "data broker" under California law. We highlight certain issues that may be created by the regulations unless they are carefully crafted to be consistent with the CCPA and existing implementing regulations. Our goal is for any new regulation to be protective of consumers while remaining workable for data brokers and the businesses and nonprofits who rely on data for mission-critical decisions and consumer and contributor engagement.

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country, including California. These companies range from small businesses to household brands, nonprofits, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product ("GDP")

[1] *See Invitation for Preliminary Comments on Proposed Rulemaking Under Senate Bill 362*, CALIFORNIA PRIVACY PROTECTION AGENCY BOARD (May 31, 2024), *available* here. *See also* California Delete Act, *available* here.

in 2020.[2] Our group has more than a decade's worth of hands-on experience it can bring to bear on matters related to consumer privacy and controls. We would welcome the opportunity to engage with the CPPA further on the points we discuss in this letter.

I. The CPPA should issue regulations that outline the procedure for validating the authority of authorized agents to act on behalf of consumers.

The California Delete Act states that the accessible deletion mechanism constructed by the CPPA must "support the ability of a consumer's authorized agents to aid in the deletion request."[3] However, the statute sets forth no guardrails to guide how the agency should ensure that requests it receives through authorized agents are expressions of consumers' *actual* choices, or that an agent *actually* received authority from the consumer to submit a request on their behalf. The proposed regulations must avoid establishing an incentive for gaming the DROP system with dictionary or "white pages" attacks by ill-intentioned or competitive actors purporting to act on consumers' requests when consumers did not in fact authorize them to act. The CPPA should issue a regulation explicitly stating that the requirements, or similar requirements, for validating authorized agents' authority to submit requests under the CCPA regulations also extend to authorized agent requests related to the deletion mechanism.

a. CPPA regulations related to validating agents' authority to act should explicitly protect consumer rights from potential abuse by intermediaries.

Under CCPA regulations, if a consumer uses an authorized agent to submit a deletion request, the business may require the agent to provide signed proof that the consumer gave the agent permission to submit the request *in addition to* asking the consumer to directly confirm their identity with the business or directly confirm that they granted the agent permission to make the request.[4] Any proposed rules to implement the California Delete Act must provide legally and functionally consistent, clear direction on the interactions between the CPPA, data brokers, consumers, and authorized agents to efficiently manage and process deletion requests made through the DROP. Accordingly, the CPPA will serve as an entrusted intermediary between consumers, authorized agents, and data brokers, facilitating deletion requests submitted through the DROP and maintaining an important clearinghouse function to ensure that requests were actually initiated by consumers, that consumers provided informed consent to authorize the agent to act on their behalf, and choices expressed through the DROP were actually desired by the consumer.

As part of the DROP, the CPPA will directly receive requests from authorized agents who claim to act on behalf of consumers. To help minimize the possibility of fraudulent requests made

[2] John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located at https://www.iab.com/wp-content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf (hereinafter, "Deighton & Kornfeld 2021").

[3] *See* Cal. Civ. Code § 1798.99.86(b)(8).

[4] *See* Cal. Code Regs. tit. 11 § 7063(a).

through agents that were not duly authorized to act by a consumer, the CPPA should draft rules that mandate that authorized agents provide signed proof of their authority to act and consumers confirm directly with the CPPA that they have authorized an agent to submit a deletion request on their behalf. This approach aligns with the authorized agent authority validation process outlined in CCPA regulations.[5] Without a robust process to verify that authorized agents have obtained evidence of consumers' genuine intent to make choices through them, these agents or market competitors could, for example, potentially submit requests to the CPPA requiring competitors to delete and opt out their datasets. The need for robust requirements to check agents' authority to submit requests on behalf of consumers warrants careful consideration.

b. The CPPA should consider a separate regulatory process to define processes for validating authorized agents' authority to act.

If the CPPA does not harmonize its authorized agent rules under the California Delete Act with existing CCPA regulations, the CPPA should ensure it issues regulations to determine a robust process to verify authorized agents' authority to act on behalf of consumers. The CPPA should potentially consider issuing such regulations through another, agent-specific regulatory process, and declining to receive requests through authorized agents until such a process is defined.

To minimize unintended results for Californians and foster consistency with requirements in other contexts, we encourage the CPPA to provide rules that explicitly prohibit agents from being able to self-certify their authority to act on behalf of a consumer. The rules should also state that informed consent to use an authorized agent is required. Authorized agents should be subject to the same requirements business and data brokers are required to meet when seeking authorization from consumers. Specifically, authorized agents should be required to acquire consumer consent to act on the consumer's behalf in accordance with the CCPA. The CCPA's definition of "consent" requires a specific, informed, and unambiguous indication of a consumer's wishes and strictly proscribes the use of general or broad terms of use, or a similar document, to obtain consent.[6] The same policy principles should be carried through in the context of authorized agent requests under the California Delete Act. In the draft rules, the CPPA should mandate evidence that consumers provided affirmative, informed consent for an agent to act on their behalf. Otherwise, there will be exposure to the risk of frivolous litigation and other unintended consequences from those seeking to exploit consumer rights for profit, rather than protecting consumers.

Instances of this type of agent behavior are playing out nationwide, most notably in relation to New Jersey's Daniel's Law and the important protections the law was intended to provide for New Jersey civil servants.[7] As enacted, the law has created unintended consequences for this

[5] *Id.* at § 7063(a)(2).

[6] Cal. Civ. Code § 1798.140(h).

[7] Daniel's Law created a new right for "covered persons"—law enforcement officers, judges, and other state officials, as well as their immediate family members in the same home—to request that any person or business stop disclosing the covered person's home address and unpublished home telephone number to others. The law also permits "authorized persons" to make requests on covered persons' behalf. New Jersey Daniel's Law, *located* here.

protected class, however. The lack of verification provisions in the law offers no avenue for companies to check if a person submitting a request is a "covered person" or an "authorized person" under the law. Companies also have no way to discern whether authorized agents who submit requests on behalf of purported covered persons are truly authorized to submit such requests. Without a reliable means to verify requests, it becomes impossible to ensure that consumers are fully aware of the authority they grant to third party agents under the law. These third parties may subsequently obscure consent provisions within the terms and conditions of other services they offer. In addition, nefarious parties can submit false requests impersonating covered persons, and companies will have no way to discern that the request is fraudulent.

In sum, the CPPA should issue regulations describing how it will validate authorized agent requests through the DROP. The CPPA should require agents to submit signed proof of their authority and require consumers to directly confirm with the CPPA that they provided requisite authority to an agent. The CPPA should prohibit agents from self-certifying such authority and require agents to obtain informed consent from consumers to submit requests through the DROP on their behalf. By including these measures in the draft rules, the CPPA can enhance consumer protection and help ensure authorized agents are acting in the interests of the consumers they represent.

II. The CCPA should issue regulations to establish safeguards for requests submitted through authorized agents.

In addition to setting forth an explicit process to verify authorized agents' authority to submit requests on behalf of consumers, the CPPA should issue regulations to create other consumer safeguards for authorized agent requests. Specifically, and as discussed in more detail below, the CPPA should issue regulations to (a) minimize the possibility of anti-competitive results from authorized agent requests; (b) ensure agents are held to the same standards that data brokers and the CPPA are held to when they describe available rights to individuals; and (c) prohibit authorized agents from making secondary uses of data they receive from consumers or charging consumers to submit requests to exercise rights that would otherwise be available to them for free.

a. The CPPA should issue regulations to deter anti-competitive gamesmanship through authorized agent requests.

Under the California Delete Act, the DROP presents an opportunity for competitive interference. Some entities may exploit the DROP for their competitive advantage. We encourage the CPPA to draft rules that reduce the risk of misuse of the DROP.

The draft rules should authorize a company to act as an authorized agent *only* if it uses personal information *solely* to fulfill consumer rights requests, perform verification functions, or engage in fraud prevention. This limitation on authorized agents is set forth in the CCPA regulations and should be carried through to apply to authorized agents under the California Delete

Act.[8] Moreover, this approach aligns with past Federal Trade Commission ("FTC") statements addressing the potential for abuse of agent-made requests in the context of the "do-not-call" registry and explaining the FTC's decision to decline to allow for requests made through such "third-party registrations."[9] In an effort to prevent "third-party abuse" of the system, the FTC coupled verification measures with a complete ban on allowing private companies or other third parties to register consumers with the national registry.[10] The same policy principles that guided the FTC's limits on third-party registrations should guide the CPPA in promulgating rules to deter anti-competitive conduct in the context of authorized agent requests through the DROP.

b. The CPPA should issue regulations that require agents to adhere to the same standards as data brokers and the CPPA when presenting choices to consumers.

Agents should be required to adhere to the same standards that businesses, data brokers, and the CPPA must observe when presenting choices and privacy rights to consumers.[11] The CPPA should issue regulations that obligate agents to offer the same choices that consumers would encounter if they accessed the DROP directly and explain the impacts and scope of privacy choices to consumers.

For example, the California Delete Act requires the deletion mechanism to "allow[] a consumer to selectively exclude specific data brokers from a [deletion mechanism] request."[12] Authorized agents should similarly be required to present the same options to consumers. Agents should not be permitted, for instance, to provide consumers with only one option to delete data from *all* registered data brokers. The CPPA must present and allow for Californians to toggle through and select or de-select specific data brokers from the list of registered data brokers that will receive a deletion request. Agents should provide consumers with equivalent options when choosing data brokers for submitting deletion requests. Since the CPPA itself must offer consumers the ability to exercise granular choices, agents must be required to do the same to effectuate the letter of the law.

In addition, the CPPA's draft rules should mandate that authorized agents must provide clear and neutral explanations of the deletion mechanism to consumers. Like the prohibition against businesses' use of dark patterns to entice or dissuade consumers from making certain choices under the CCPA,[13] authorized agents should similarly be required to refrain from using sensational language or coercive tactics to encourage consumers to use the deletion mechanism. Agents should be required to accurately explain the scope and impact of privacy choices to consumers. The draft rules should safeguard against agents using manipulative language that distorts or exaggerates the consequences of utilizing or foregoing use of the DROP.

[8] *See* Cal. Code Regs. tit. 11, § 7063(d).

[9] *See* Federal Trade Commission, *Final Amended Rule: Telemarketing Sales Rule*, 68 Fed. Reg. 4580, 4639 (Jan. 29, 2003).

[10] *See* Federal Trade Commission, *Q&A: The National Do Not Call Registry*, located here.

[11] *See* Cal. Code Regs. tit. 11, § 7010.

[12] Cal. Civ. Code § 1798.99.86(a)(3).

[13] *See id.* at § 1798.185(20)(C)(iii). *See also* Cal. Code Regs. tit. 11, § 7004(b).

c. The CPPA should issue regulations that prohibit agents from making secondary uses of data they receive from consumers or charging consumers.

The draft rules should explicitly prohibit authorized agents from making secondary uses of the data they receive from consumers through their role as an authorized agent or charging consumers for using or submitting requests to the DROP, ensuring that consumers are not misled into paying for a service they could otherwise perform independently at no cost. Agents should be required to use information they receive from consumers in the context of DROP requests solely to facilitate requests through the DROP. In addition, under the California Delete Act, the CPPA may not charge consumers for making deletion requests through the DROP.[14] Similarly, authorized agents should not be permitted to profit from consumers by submitting requests on their behalf.

III. The CPPA should issue regulations allowing data brokers to independently verify consumer deletion requests made via the DROP and permitting data brokers to obtain information necessary to effectuate opt-out requests.

The CPPA should draft rules that permit data brokers to independently verify consumer requests to ensure consumers are the individuals seeking to exercise rights under the law. The draft rules must allow data brokers to verify that they are executing deletion requests related to the personal data of the individuals making the requests to avoid "adversely affect[ing] the rights and freedoms of other natural persons."[15]

Specifically, according to the CCPA, "[t]he rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other natural persons. A verifiable consumer request… to delete a consumer's personal information pursuant to Section 1798.105… shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person."[16] The Final Statement of Reasons ("FSOR") discussing the original CCPA regulations expressly acknowledged issues associated with effectuating consumer rights on personal information associated with the wrong consumer in the context of households.[17] The FSOR noted that the California Attorney General added certain requirements to address issues with household requests implicating privacy concerns of household members who may not want personal information deleted in response to a household request to delete.[18] Amendments to the CCPA via the California Privacy Rights Act of 2020 addressed the concern associated with effectuating consumer rights in ways that would impact the rights and freedoms of others in the context of households by squarely stating that requests to delete do not apply to household data.[19] In some cases, additional measures may be necessary to verify a request received via the DROP to help ensure a request is applied to the personal information

[14] *See* Cal. Civ. Code § 1798.99.86(b)(5).

[15] *Id.* at § 1798.145(k).

[16] *Id.*

[17] *See* Final Statement of Reasons for Proposed Adoption of CCPA Regulations at 44 (Jun. 1, 2020), located here.

[18] *Id.* at 44-45.

[19] Cal. Civ. Code. 1798.145(p).

associated with the correct person to avoid adversely affecting the rights and freedoms of other natural persons.

Moreover, different data brokers operate by processing different types of personal information. For example, while one data broker may handle personally identifiable information, such as names and addresses, another might exclusively process pseudonymous identifiers not directly tied to consumer identities. Considering the diverse landscape of data brokers and what they collect, a verification process that allows data brokers to independently verify consumer requests against the personal information they actually maintain would help ensure accurate action is taken in response to a consumer's request while safeguarding the rights and freedoms of all parties involved.

In addition, under the California Delete Act, if a data broker denies a consumer's deletion request on the ground that it is unverifiable, the data broker must process it as a request to opt out of the sale or sharing of the consumer's personal information under the CCPA.[20] Even though consumer opt out requests need not be verified pursuant to California law, data brokers must still have the means to locate a consumer within their systems in order to facilitate the alternative opt-out right. The CPPA's regulation should take this reality into account. Some measure of personal information will need to be collected and accurately matched to personal information in a data broker's systems to effectuate opt-out rights. The CPPA should permit data brokers to receive such information in the context of the DROP so they can locate the right consumer in their systems to process an opt-out request.

IV. The CPPA should issue regulations to clearly explain the scope of the deletion mechanism to consumers.

Under the California Delete Act, data and entities subject to certain federal laws are exempt from the scope of the accessible deletion mechanism.[21] In addition, the statute includes other relevant exceptions for requests submitted through the DROP, such as exceptions relating to maintaining data for security and integrity purposes.[22] The CPPA should ensure that it makes these exemptions clear to consumers on the main webpage that houses the DROP. Consumers should be aware of the scope of their requests and should be appropriately informed of relevant protections under law. For example, anti-fraud products and services play a crucial role in protecting consumers and ensuring their safety from fraudulent activities and scammers. Companies rely on the use of data to verify the identities of customers and keep them safe from fraud. Consumers should be assured that deletion requests made through the DROP will not eliminate the data necessary for them to receive the benefits of these anti-fraud and identity theft services, as such an outcome would not only be detrimental to consumer safety but also contradict consumers' expectations and desires for robust security measures.

[20] *See id.* at § 1798.99.86(c)(1)(B).
[21] *Id.* at § 1798.99.80(c).
[22] *Id.* at §§ 1798.99.86(c)(1)(B), (D); (c)(2).

V. The CPPA should ensure its regulations strictly adhere to the statutory definition of a "data broker" under California's data broker registry law.

The CPPA has publicized draft regulations indicating that it is contemplating changes to the legally defined term "data broker" under California law.[23] The CPPA should ensure its draft rules align with the definition of "data broker" under California's data broker registration law to ensure consistency in implementation and enforcement.[24] Any changes to the definition may not broaden or materially alter the definition established by the legislature via statute.

The California Delete Act defines a data broker as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."[25] The CPPA is considering defining "direct relationship" to mean a consumer's intentional interaction with a business "for the purpose of obtaining information about, accessing, purchasing, using, or requesting the business's products or services within the preceding three years."[26] In addition, according to the proposal, "a consumer does not have a 'direct relationship' with a business if the purpose of their engagement is to exercise any right described under [the CCPA], or for the business to verify the consumer's identity. *A business is still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer*."[27]

This definition does not align with the original intent of the data broker registration law.[28] In the preamble of the data broker registration bill, the California legislature found that "there are important differences between data brokers and businesses with whom consumers have a direct relationship. Consumers who have a direct relationship with businesses… may have some level of knowledge about and control over the collection of data by those businesses, including: the choice to use the business' products or services, the ability to review and consider data collection policies, the ability to opt out of certain data collection practices, the ability to identify and contact customer representatives, and the knowledge necessary to complain to law enforcement."[29] As proposed, the definition of "direct relationship" would mean the term "data broker" would likely cover every business in California, as "sale" is defined extremely broadly in the CCPA and virtually every business collects personal information from third-party sources other than the consumer themself. We urge the CPPA to draft rules that do not incorporate this proposed definition of "direct relationship," which goes beyond the scope and intent of the law.

* * *

[23] *See* CPPA Board Meeting, Agenda Item 4: Data Broker Registration Draft Text (May 10, 2024), *available* here.
[24] *See* Cal. Civ. Code § 1798.99.80(c).
[25] *Id.*
[26] *See* CPPA Board Meeting, Agenda Item 4: Data Broker Registration Draft Text (May 10, 2024), *available* here.
[27] *Id.* (emphasis added).
[28] *See* California AB 1202 (Reg. Sess. 2019), Sec. 1(g), located here.
[29] *Id.*

Thank you in advance for your consideration of these preliminary comments.

Sincerely,

Christopher Oswald
EVP for Law, Ethics & Govt. Relations
Association of National Advertisers
[redacted]

Alison Pepper
EVP, Government Relations & Sustainability
American Association of Advertising Agencies, 4A's
[redacted]

Lartease Tiffith
Executive Vice President, Public Policy
Interactive Advertising Bureau
[redacted]

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
[redacted]

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
[redacted]

CC: Mike Signorelli, Venable LLP
Allaire Monticollo, Venable LLP
Matt Stern, Venable LLP

Comments of Consumer Reports, Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC) and Privacy Rights Clearinghouse (PRC)
In Response to the
California Privacy Protection Agency's
Invitation for Preliminary Comments On
Proposed Rulemaking Under Senate Bill 362

By

Matt Schwartz, Policy Analyst, Consumer Reports
Justin Brookman, Director of Technology Policy, Consumer Reports

June 25, 2024

The undersigned organizations appreciate the opportunity to provide feedback on the California Privacy Protection Agency's (CPPA) Invitation for Preliminary Comments on Proposed Rulemaking Under Senate Bill 362 (the Delete Act). We thank the CPPA for initiating this proceeding and for its other efforts to protect consumer privacy.

We are pleased that the Agency is moving quickly to implement critical provisions of the Delete Act, which focuses on the inherently privacy-eroding data broker industry that has a well-documented history of abusive and harmful business practices.[1] The law remedies an oversight in the California Consumer Privacy Act (CCPA), whereby deletion rights only apply to "data about the consumer which the business has collected *from the consumer*" (emphasis added), arguably opening up the interpretation that deletion rights do not apply to entities that collect information about consumers indirectly, as is the business model of many data brokers. It addresses the threshold issue of how deletion rights ought to apply to an industry that many consumers likely do not even know exists, let alone how they might locate and exercise their rights with the specific data brokers that may have collected their personal information.

Importantly, with the mandate that the Agency create an "accessible deletion mechanism" that allows consumers to delete all of their personal information held by the state's registered data brokers in a single action, the law adopts the perspective that many consumers are likely to want to delete their information from the data broker industry as a whole, and that the process for doing so should be as seamless as possible. Now, the Agency seeks comments on how it is to operationalize this system.

We describe our views on each of the potential areas for rulemaking in the course of providing answers to the questions posed by the CPPA in its invitation.

I. Verifiable Consumer Requests

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.

[1] See, e.g., Joseph Cox, The Secret Weapon Hackers Can Use to Dox Nearly Anyone in America for $15, 404 Media (Aug. 22, 2023), https://www.404media.co/the-secret-weapon-hackers-can-use-to-dox-nearly-anyone-in-america-for-15-tlo-usinfosearch-transunion/;
Douglas MacMillan, Data Brokers are Selling Your Secrets. How States are Trying to Stop Them, Washington. Post (Jun. 24, 2019). https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-yoursecrets-howstates-are-trying-stop-them/; Jon Keegan and Joel Eastwood, From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found
650,000 Ways Advertisers Label You, The Markup, (June 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you
.

a. *What should constitute a “verifiable consumer request”?*

General Views

In general, our view is that the Agency should create a low bar for consumers to meet in terms of identity verification. The Delete Act was written to focus on data brokers that primarily deal in the creation of data dossiers and individualized marketing profiles, typically without the knowledge or explicit consent of consumers. It only applies to data brokers that “knowingly collect and sell to third parties the personal information of a consumer with whom the business does not have a direct relationship,”[2] ruling out other types of businesses with direct consumer relationships that nonetheless collect and sell user information (e.g. tech giants like Facebook and Google), but for which a universal deletion mechanism may be too blunt an instrument. For example, while these consumer-facing entities harbor deep tranches of personal data and sell inferences about consumers’ behavior, they also maintain information a consumer may have directly provided and may reasonably want to preserve (e.g. important user profile information, photos, and documents).

Beyond that, the Delete Act exhaustively excludes from coverage other types of data that may provide some sort of societal benefit, or, were they to be deleted, could potentially prove harmful to a consumer; the Delete Act exempts any entity to the extent that is covered by FCRA, GLBA, the Insurance Information and Privacy Protection Act, CMIA, and HIPAA, as well as any publicly available data as defined in CCPA.[3] Given that these limitations scope the law to seemingly only cover data brokers’ consumer profiles collected from private sources, such as consumer web searches, apps and online behavior, preferences, geolocation, and inferences derived from these factors, it appears that the risk of harm from mistakenly deleting a consumer’s record is low, while the risk of harm of *not* deleting a consumer’s record upon their request is high.

Direct Consumer Verifications

With this in mind, when the request comes directly from a consumer visiting the accessible deletion mechanism, we believe the request should be considered verifiable when either an email address or a phone number can be authenticated by the Agency. In our view, this authentication method strikes the best balance between ease of consumer use, efficacy, and privacy considerations. Consumers have grown accustomed to authenticating themselves in this manner,[4] and many data brokers already commonly request these identifiers for purposes of effectuating do not sell requests under CCPA.[5] While we considered the merits of additional

[2] Delete Act, Section 1(c), https://legiscan.com/CA/text/SB362/2023
[3] *Id* at Section 1(c)(1-4); Section 1(a) (deferring to CCPA’s definition of personal information).
[4] Chrysta Cherrie, 2FA Statistics: 2FA Climbs, While Password Managers and Biometrics Trend (noting a rising trend in survey respondents who have used two-factor authentication and that SMS and email were the most common second factors), Duo Labs (September 14, 2021), https://duo.com/blog/the-2021-state-of-the-auth-report-2fa-climbs-password-managers-biometrics-trend
[5] Maureen Mahoney, California Consumer Privacy Act: Are Consumers’ Digital Rights Protected? (finding that email address was the most commonly requested identifier, followed by name, address, and phone number), Consumer Reports Digital Lab, (Oct. 1, 2020),

identifiers common to data broker profiles, such as home address, we view this factor to be both impracticable (likely requiring a time consuming mail correspondence) and potentially more privacy invasive than either phone or email verification. Given these considerations, we do not believe the universal deletion mechanism needs to allow for home address verification, though consumers should be able to submit current and past addresses as part of their deletion request.

One of the primary challenges here is the inherent informational asymmetry that exists between consumers and data brokers (as well as the CPPA) — how are consumers to know exactly what information a given data broker *truly* needs in order to successfully process a deletion request? While the Delete Act will increase the amount of information data brokers must share about their data collection practices,[6] they still aren't required to share the key identifiers that they collect or how their data profiles are structured. The CPPA should seek to remedy that with this rulemaking by requiring each data broker to share with the CPPA the minimum necessary set of identifiers able to identify a majority of their consumers.

One of the harms we've encountered when data brokers are allowed to determine the parameters for verification is that they will use the asymmetry to their advantage, requesting information that is clearly not needed to carry out the request. For example, even though Consumer Report's authorized agent, Permission Slip, provides first and last name, verified phone number, verified email, address, signed authorized agent letter, and more with each consumer request, one data broker routinely asked for consumers' birth dates on top of this information. Then, when consumers refused to provide the additional information, the data broker would complete the request regardless — implying that the information was never actually required. Consumer Reports also documented similar abuses during its study of the usability of CCPA rights, finding examples of data brokers requiring consumers to take a selfie or download a third-party app in order to verify identity or applicability of CCPA rights.[7] In some cases, these processes were so onerous that they had the effect of preventing consumers from completing their rights request. On the other hand, if a consumer does not provide enough information, or the right type of information, a data broker acting in good faith may well not be able to complete the request.

Data Broker Treatment of Verified Requests

Many data brokers link several identifiers to a single consumer's data profile (e.g. phone number, email, address, advertising ID). As discussed above, a consumer's request should be considered verifiable when just one one of those identifiers (phone or email) has been authenticated by the consumer. Upon receiving a verified request, data brokers should be

https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf

[6] *Id at* Section 3(b)(2)

[7] Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Digital Rights Protected? Consumer Reports Digital Lab, (Oct. 1, 2020), https://advocacy.consumerreports.org/wpcontent/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf

required to delete all of the corresponding information reasonably likely to be associated with the consumer. A “reasonably likely” standard recognizes that there may be a degree of probabilistic linkage in data broker records but that it might be undesirable for the agency to articulate an arbitrary standard of certainty above which deletion should be required (i.e. should deletion be required when data brokers are 60 percent confident of linkage, or 75 percent certain of linkage)?

Additionally, the CPPA should clarify that the consumer’s initial submission of their verified request, either through the accessible deletion mechanism directly or through their authorized agent, should mark the end of the consumer’s responsibility to verify themself or provide request information. Data brokers should not be allowed to respond to universal deletion requests by contacting consumers to ask for additional verification or further information to complete the deletion request. The purpose of a universal deletion mechanism is to reduce the burdens on consumers — a benefit that would be largely eroded if data brokers were permitted to respond to universal deletion requests with individualized responses for additional information.

Device IDs

Some data brokers *only* amass consumer profiles using device identifiers, such as IP address, mobile advertising IDs, or cookies, which may make it more difficult for consumers to send a successful request using more traditional personal identifiers like email or phone alone. Though, in some cases, consumers could theoretically look up their device IDs and manually enter them into a field on the accessible deletion mechanism website, this may prove burdensome for consumers[8] or difficult to authenticate. The CPPA should consider how it could provide an alternative process to address deletion requests for this subset of data brokers, potentially by automatically capturing and including IP address or mobile advertising ID with a consumer’s request, for example, when a consumer fills out a deletion request using their mobile device. Such a framework would have the benefit of being self-authenticating, reducing additional burden on consumers. While this process may not be capable of capturing domain-specific identifiers, like cookies, the CCPA’s universal opt-out mechanism provisions at least allow consumers to suppress cookie-based tracking in the interim while platforms increasingly move toward the deprecation of third-party cookies altogether.[9]

Verifications Through Authorized Agents

Consumers should also be able to authenticate their identity and send a verifiable request through their authorized agent of choice. Some authorized agents already have robust verification measures in place that meet or exceed CCPA’s existing requirements. For example, in addition to the signed permission required by the CCPA Rules (Section 7063(a)), Permission

[8] *Id* at 24.
[9] See, e.g., Tina Moffett, Google Makes Good On Its Resolution To Deprecate Third-Party Cookies In 2024, Forrester, (January 4, 2024), https://www.forrester.com/blogs/google-makes-good-on-third-party-cookie-deprecation/?utm_source=forbes&utm_medium=pr&utm_campaign=b2cm

Slip currently requires consumers to verify their email address and phone number as part of their onboarding process.[10] In order to provide further certainty about the standing of authorized agents, the CPPA could create a registry of trusted authorized agents that must meet similarly robust standards of identity verification and other indicia of trustworthiness. Those included in the registry could then send consumer requests without additional verification.[11]

II. Privacy Protecting

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?"

Data Minimization

As discussed earlier, one of the best ways to improve consumer privacy is to require that consumers only submit the minimum information possible with their deletion request (i.e. verified phone or email). However, the CPPA may also be considering what optional fields consumers should be allowed to fill out in order to increase their chances of a successful request. In our view, consumers should be able to augment their deletion request with additional identifiers like their home address, date of birth, middle name, maiden name, and alternative emails and phone numbers. However, we do not believe that CPPA should permit the submission of any government identifiers (e.g. social security numbers, passport numbers, driver's license scans) or biometric identifiers with consumer requests. From a data security standpoint, collection of this information creates an unacceptable degree of risk for CPPA when weighed against the risk of mistaken deletion. It would also create the risk of improper use by data brokers, whose business model inherently incentivizes them to create the most accurate consumer profiles possible (notwithstanding the purpose limitation principle discussed below). Improper proliferation of biometric identifiers, for example, can cause irrevocable harm to consumers considering that they cannot be changed when they are compromised.[12]

Purpose Limitation

Though the CCPA already includes a provision that requires that businesses solely use personal information collected from the consumer in connection with the business' verification of the deletion request for that purpose and for no "unrelated purposes", the CPPA should clarify in its

[10] Tara Claesgens, How does Permission Slip work?, Consumer Reports Innovation Lab, (November 16, 2023), https://innovation.consumerreports.org/how-does-permission-slip-work/

[11] CCPA Regulations, Section 7063(b), (noting that receiving Power of Attorney prevents a business from requiring the consumer to verify their own identity directly with the business or directly confirm with the business that they provided the authorized agent permission to submit the request), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf

[12] Woodrow Hartzog, Facial Recognition Is the Perfect Tool for Oppression, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for- oppression-bc2a08f0fe66.

rules that data brokers cannot use *any* personal information (including that which was not used for verification purposes) provided as part of a consumer's deletion request for any other purpose aside from honoring the request.[13] Anecdotally, in Consumer Reports' experience as an authorized agent, some entities appear to be misusing consumer data submitted as part of a request for marketing purposes. In some instances, users and employees have reported receiving marketing emails from entities where the person's only known interaction with the company was submitting a rights request. The marketing emails appeared shortly after the submission of the request. Consumer Reports experienced a similar phenomenon during its study of data brokers' opt-out processes under CCPA; a study author was placed on data broker X-Mode's newsletter despite her only interaction with the company being her opt-out request.[14]

Data Security

The Delete Act states that the CPPA shall establish an accessible deletion mechanism that "implements and maintains reasonable security procedures and practices".[15] At a minimum this should include encryption of the consumer's submission of personal information to the accessible deletion mechanism in transit and at rest. The CPPA should also consider how an API-based implementation of the Delete Act could advance data security objectives.[16] Programmatically exchanging rights requests could help avoid the need to maintain a widely accessible, central registry of consumer records, which would likely serve as a high-value target for hackers. Theoretically, the API could also be structured to send request information in an individualized format for each data broker, so that they only receive the information necessary for them to carry out the request. For example, a data broker that only collects device IDs would not be sent consumer email addresses or phone numbers, helping minimize the potential for misuse described above. Consumer Reports' Permission Slip app has successfully experimented with sending consumer rights requests programmatically via the Data Rights Protocol.[17]

b. In what privacy-protecting ways can data brokers determine whether an individual has submitted a deletion request to the Agency?

As discussed earlier, data brokers should be required to delete the entirety of a consumer's profile upon matching one of the key authenticated identifiers (phone or email). This framework should reduce the amount of data that brokers are looking for in the first place. Upon deleting the consumer's record, the broker should be allowed to retain certain identifiers for the purposes

[13] CCPA Section 1798.130(a)(7)

[14] Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Digital Rights Protected? (pg. 34-37), Consumer Reports Digital Lab, (Oct. 1, 2020), https://advocacy.consumerreports.org/wpcontent/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf

[15] Delete Act, Section 6(a)(1), https://legiscan.com/CA/text/SB362/2023

[16] Ryan Rix, Securing and Standardizing Data Rights Requests with a Data Rights Protocol, PEPR '23, (September 11, 2023), https://www.usenix.org/conference/pepr23/presentation/rix

[17] Ginny Fahs, Announcing a Stable Version of the Data Rights Protocol, Consumer Reports Innovation Lab, (September 12, 2023), https://innovation.consumerreports.org/announcing-a-stable-version-of-the-data-rights-protocol/

of maintaining a suppression list (subject to strict purpose limitation requirements). These identifiers should be further limited to include only those the data broker reasonably expects to collect in the future. As discussed earlier, automating the communication of rights requests also could protect consumer privacy. Instead of querying a central database, brokers could automatically receive requests personalized to their verification needs, potentially reducing the amount of personal data they have access to.

III. Status of Request

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"?*

The CPPA should ensure that the accessible deletion mechanism is capable of providing clear status updates to the consumer. Again, the benefit of the universal deletion mechanism is its centrality — consumers should be able to use the mechanism as a one-stop-shop for their data broker deletion requests, and data brokers should not be permitted to contact consumers with status updates outside of the system.

There are several components we consider essential to a status update. Most simply, the agency should allow the consumer to query the accessible deletion mechanism to determine which of their personal data were sent to which data brokers. Consumers should be able to subsequently update the data fields if they desire or submit multiple requests if they possess multiple emails or phone numbers they wish to append to their request. The CPPA should also require data brokers to confirm to the accessible deletion mechanism when they've received the initial deletion request and intend to take action, when they've completed a request, or when they couldn't match the exact consumer and thus processed the request as an opt-out of sale or sharing, as required under the Delete Act.[18] This will allow consumers to query the accessible deletion mechanism and confirm how many of the brokers had a match for their submitted data.

In the event that a request is denied, data brokers should include specific information explaining why. For example, data brokers should detail whether the request was denied because the data broker couldn't match the provided identifiers with data in their system, the information is protected under an exemption (clearly explaining which exemption they are relying on), they believed the request was fraudulent, or any other grounds for denial. Data brokers should provide all status updates to the CPPA as soon as reasonably possible after taking an action related to the status update.

IV. Consumer Experience

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

[18] Delete Act, Section 6(c)(1)(B), https://legiscan.com/CA/text/SB362/2023

information 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?*

Consumers benefit most from universal controls when they are simple and easy to use. As mentioned throughout, CPPA's rules should clarify that a consumer should only be required to interact with the universal deletion mechanism in order to complete their requests and check for status updates. We note that the data broker industry advocated the opposite approach through legislation they sponsored earlier in the legislative session, by requesting the ability to directly contact consumers using the accessible deletion mechanism or when they used an authorized agent to send a universal deletion request.[19] This could result in consumers receiving hundreds of emails upon submission of a universal deletion request, with data brokers asking consumers to provide additional information in order to "complete the request," to rescind the request, or to whitelist the specific data broker. From the consumer's perspective, the initial request should be the end of their interaction with the accessible deletion mechanism, unless they wish to return to check on the status of their request or append their request with more information.

Additionally, a consumer's decision to use an authorized agent to send a universal request should be respected. Permission Slip regularly encounters businesses that attempt to circumvent them by responding to requests by directly contacting the consumer, often asking consumers to resubmit request information originally submitted by Permission Slip. This behavior typically confuses or angers consumers who have gone out of their way to designate authority to the authorized agent. The forthcoming rules should clarify that, to the extent that communication is ever necessary as a result of a universal deletion request, data brokers must correspond with authorized agents exclusively when consumers have chosen to exercise their rights in this manner.

****

We thank the California Privacy Protection Agency for its consideration of these points, and for its work to secure strong privacy protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Matt Schwartz [redacted] or Justin Brookman [redacted] for more information.

[19] Senate Bill 1076, Section 2 (b)(8)(H); Section 2 (b)(11), https://legiscan.com/CA/text/SB1076/id/2925501

To: Data Broker Unit,

On behalf of LiveRamp, please accept this email as a LiveRamp's response to invitation for comments on proposed rulemaking under Senate Bill 362.

1. Verifiable Consumer Requests

a. What should constitute a "verifiable consumer request"?

Response:
A verifiable consumer request under the Delete Act should prioritize both security and user privacy. Here's how we can achieve this:

Modern Secure Sharing:

Employing a modern data clean room equipped with technologies like Multi-Party Computation (MPC) allows for secure data comparison during verification without any data movement. This protects sensitive consumer information throughout the process.

Multi-Layered Verification:

A combination of methods strengthens identity verification. This may include:

- **Knowledge-Based Authentication (KBA):** Challenge-response questions covering a range of personal details like name, address variations, and known relationships.
- **Multi-Factor Authentication (MFA):** Sending a one-time verification code to a user's registered phone number or email for an extra layer of security.
- **Optional Document Verification:** For high-risk deletion requests, allowing users to submit scanned copies of government-issued IDs for additional verification (ensure secure document handling procedures are in place).

Balancing Security and Privacy:

We understand user concerns regarding sensitive information like the last four digits of Social Security Numbers (SSN). Instead, consider alternatives like date of birth variations or unique account identifiers for verification. Additionally, offering consumers the option to download a personal copy of their data before deletion addresses concerns about permanent loss.

Preventing Misuse and Addressing Email Limitations:

The verification process should be robust enough to prevent unauthorized deletion attempts. Solely relying on email addresses for verification may not be sufficient as they can be shared within households. We can address this by:

- Implementing mechanisms to detect and flag suspicious deletion requests.
- Allowing users to verify deletion requests through alternate channels like phone numbers associated with their accounts.

Transparency and User-Friendliness:

- We will clearly communicate the verification process to users, explaining the rationale behind each step and the data used for verification.
- A dedicated and user-friendly channel (web form, phone line) will be established for submitting data deletion requests.

Risk-Based Approach and Timeliness:

- The verification process may be tailored based on the type and sensitivity of data being requested for deletion. Higher risk data may require stricter verification steps, adhering to a risk-based approach.
- We will set reasonable time limits for responding to data deletion requests, as mandated by the upcoming Delete Act.

2. Privacy-Protecting Submission Mechanisms

a. How should a consumer securely submit information in a “privacy-protecting way?”

Response:
Consumers should be empowered to submit deletion requests with confidence in the security of their personal information. Here are key elements for a privacy-protecting submission mechanism:

- **End-to-End Encryption:** Secure Socket Layer (SSL)/Transport Layer Security (TLS) encryption protects all communication channels during the deletion request process. This ensures data remains confidential in transit, preventing unauthorized access or interception.
- **Multi-Factor Authentication (MFA):** Implementing MFA adds an extra layer of security by verifying user identity beyond a simple password. This could involve a combination of:
    - **Something the user knows:** Password, PIN, security questions
    - **Something the user has:** Authentication app, security token
    - **Something the user is:** Fingerprint, facial recognition (optional, depending on risk)
- **Confidential Computing Environments:** Leveraging technologies like secure enclaves or hardware security modules (HSMs) ensures sensitive information is processed and stored within a highly secure, isolated environment. This further minimizes the risk of data breaches or unauthorized access.

Beyond Technology: Transparency and User Control

In addition to technical safeguards, transparency and user control are crucial for a privacy-protecting submission mechanism:

- **Clear Instructions:** Provide clear and accessible instructions on the deletion request process, outlining the information required and how it will be used.
- **User Control Over Data:** Allow users to review and confirm the information they submit before finalizing the deletion request.
- **Confirmation and Status Updates:** Provide confirmation upon successful submission and keep users informed about the progress of their deletion request.

b. In what privacy-protecting ways can data brokers determine whether an individual has submitted a deletion request to the Agency?

Response:

Data brokers can leverage privacy-enhancing technologies (PETs) to determine if an individual has submitted a deletion request to the Agency, without directly accessing personally identifiable information (PII). Here are two potential approaches:

1. **Pseudonymous Matching via Data Clean Rooms:**
    - Data brokers could utilize an intermediary with a secure data clean room environment.
    - The Agency would send a hashed and pseudonymized identifier (representing the deletion request) to the clean room.
    - Data brokers would contribute their own pseudonymized consumer data sets to the clean room.
    - Secure computations within the clean room would determine a match between the deletion request and the data broker's data, without revealing any PII.
2. **Authorized Agent with Secure Disclosure:**
    - The Agency could designate a trusted, independent third party as an authorized agent.
    - Consumers would submit deletion requests to this agent.
    - The agent would verify the request and generate a unique token linked to the deletion request.
    - The Agency would share this token with data brokers, allowing them to verify its validity without revealing the consumer's identity.

Benefits of these Approaches:

- **Privacy-Preserving:** Both methods ensure data brokers receive only confirmation of a deletion request, not the individual's PII, protecting consumer privacy.
- **Efficiency:** Utilizing existing data clean room infrastructure or a designated agent streamlines the process for data brokers to comply with deletion requests.
- **Scalability:** These approaches can handle large volumes of deletion requests effectively.

Additional Considerations:

- **Standardized Protocols:** Developing standardized protocols for data exchange and verification between the Agency, intermediaries, and data brokers is crucial for smooth implementation.
- **Security Measures:** Robust security measures within data clean rooms and secure communication channels are essential to protect data integrity and confidentiality.

3. Status of Requests

a. What information should be included in the "status of the consumer's deletion request"?

Response:

The status update for a consumer's deletion request should provide clear and informative details throughout the process.Here are key elements to consider:

- **Confirmation of Receipt:** A clear confirmation message acknowledging the consumer's deletion request and a unique reference number for tracking purposes.
- **Final Confirmation:** A clear notification upon successful deletion, including confirmation of the data types deleted and any residual data that may remain due to legal or regulatory requirements.

Additional Considerations:

- **Accessibility:** Provide status updates through multiple channels preferred by consumers, such as email, secure online portal, or phone.
- **Language Options:** Offer status updates in multiple languages to cater to a diverse user base.
- **Data Retention:** Clearly explain the data retention policy for deletion request logs, ensuring user privacy after the process is complete.

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.)?

Response:

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?

Response:

At LiveRamp, we prioritize fulfilling CCPA requests within the mandated timeframe (currently 45 days). Our resources are currently dedicated to ensuring a timely completion rate for all submitted requests.

While we don't currently offer a dedicated system for consumers to track the status of their CCPA requests beyond an initial confirmation of receipt, consumers can always submit a support ticket if the timeframe for a response has been exceeded. Our support team will be happy to investigate the status of the request and provide an update.

We understand the importance of transparency and are actively exploring ways to enhance our CCPA request process.This may include the development of a dedicated consumer portal for status tracking in the future.

Here's a summary of the current process:

1. Consumer submits a CCPA request.
2. LiveRamp confirms receipt of the request via email.
3. LiveRamp processes the request within the mandated timeframe.
4. Consumer receives notification upon completion of the request.
5. If the timeframe is exceeded, consumers can submit a support ticket for a status update.

4. Consumer Experience

a. What should the Agency consider with respect to the consumer experience?

Response:

The Agency should prioritize a comprehensive user-centric approach when designing the deletion mechanism. Here are key considerations that go beyond deletion:

- **Intuitive Interface:** A user-friendly interface with clear navigation and step-by-step guidance simplifies the deletion process, data portability requests, and potential reversal options.
- **Accessibility Features:** WCAG compliance ensures accessibility for users with disabilities for all functionalities,including deletion, data portability, and reversal options.
- **Multilingual Support:** Offering instructions, FAQs, and explanations in multiple languages removes language barriers and empowers a diverse consumer base.
- **Transparency and Education:** Clear and concise information about the deletion process, data portability options,potential limitations, and any considerations for reversing a deletion fosters trust and informed decision-making.
- **Multiple Support Channels:** Providing options for phone, email, and chat support ensures consumers can get assistance regardless of their preferred communication method for deletion, data portability, or reversal inquiries.

Additionally, the Agency should consider:

- **Data Portability Options:** Allowing consumers to easily download a copy of their personal data before deletion empowers them to retain control and potentially use it elsewhere.

- **Reversal Options:** While the core function might be deletion, consider exploring mechanisms for consumers to potentially flag or archive data before deletion, allowing them to potentially recover it within a specific timeframe (balancing the right to be forgotten with potential retrieval needs).

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?

Response:
The Agency can promote widespread participation by implementing these strategies:

- **Public Awareness Campaigns:** Educate consumers about their rights and the deletion mechanism's availability,including data portability options and any considerations for reversing a deletion. Utilize diverse communication channels (television, radio, social media) to reach a broad audience.
- **Community Partnerships:** Collaborate with community organizations and advocacy groups to reach underserved populations who may not have easy access to online resources or awareness of their data privacy rights.
- **Mobile-Friendly Design:** Recognize the dominance of mobile devices and ensure the mechanism is optimized for smartphones and tablets, encompassing deletion, data portability functions, and any potential reversal options.
- **Multilingual Resources:** Provide educational materials and FAQs in multiple languages to cater to California's diverse population.
- **Offline Options:** Offer alternative channels for submitting deletion requests, data portability requests, and potential reversal inquiries, such as downloadable mail-in forms or designated locations for in-person assistance. This caters to those with limited internet access or those who prefer non-digital methods.

5. Additional Comments: Accessible Deletion Mechanism

LiveRamp recognizes the importance of the Agency's efforts to establish an accessible deletion mechanism for California consumers. We believe a well-designed mechanism can empower consumers with control over their personal data while fostering a healthy digital ecosystem.

Collaboration for Effective Implementation:

LiveRamp is committed to collaborating with the Agency to ensure the deletion mechanism is implemented effectively. We believe the following considerations are crucial for achieving this goal:

- **Balancing Consumer Control and Economic Impact:** Balancing the need for consumer control over data with the legitimate uses of data for economic purposes. This includes recognizing the role third-party data plays in supporting a competitive advertising landscape and innovations in privacy enhancing technologies.
- **Preserving Competition:** Designing the mechanism to avoid inadvertently hindering competition in the marketplace. It's important to ensure small, medium, and large businesses can continue to leverage data responsibly alongside the largest dominant 1st-party platforms.
- **Preventing Misuse:** Establishing safeguards to prevent malicious actors from exploiting the deletion mechanism to manipulate the market.

- **Future-Proofing Regulations:** Developing regulations with flexibility to adapt to evolving technologies and privacy-enhancing solutions.
- **Transparency and Clear Guidelines:** Providing clear guidelines for data brokers, including verification processes and secure data handling practices, to ensure the mechanism is implemented effectively.

Considerations for Consumer Protection:

- **Mitigating Potential Risks:** While deletion is a right, it's important to consider potential unintended consequences, such as increased risks of fraud if certain data becomes unavailable for identity verification purposes.
- **Consumer Education:** Supporting consumer education initiatives to ensure individuals understand their data privacy and portability rights and can make informed choices about data deletion.

LiveRamp is committed to working with the Agency to develop a solution that prioritizes consumer privacy, fosters innovation, and protects a competitive digital marketplace.

From: [redacted]
To: DataBrokers@CPPA
Subject: Fwd: CPPA to Hold Virtual Preliminary Stakeholder Session Regarding Data Broker Accessible Deletion Mechanism
Date: Tuesday, June 25, 2024 7:10:53 PM

This Message Is From an Untrusted Sender
Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Please accept this delayed input on the modern job applicant perspective:

1a Required: first name, last name and one of the following options: phone number (to receive texts) or email address or mailing address. This data should list on a credit report. Perhaps allow in the process for the consumer to pick which of the top three bureaus to pull verification information. Perhaps take note from the Free Annual Credit Report website's process. Make the process as easy as requesting a fraud alert or credit freeze.

1c My experience in almost all requests (to original entities e.g. prospective employers, past employers) to learn which entities my PII has been shared with and to request my PII to be deleted have been met with a response request for me to submit more PII than the submission to the original entity asked of me (such as a phone number, email address, mailing address, last four of my SSN or driver's license number). The request puts the consumer in an even more compromised data privacy compromised position. Often I do not fulfill the process for fear of creating even more exposure for myself.

2 Given the proliferation of data breaches, exfiltrated data, and the basic response of an original entity offering compensatory free credit monitoring, how about the CA DMV end its own data broker division to spin-off a division that receives

3ab. Include delivery/ response date, request confirmation number, and website page URL to get timely status including situation-specific explanation of delay

4ab In the job application process, application platforms can evolve to have (for CA residents) an option to begin the data deletion process. The grand majority of applicants do not get selected to be hired. In an ideal situation, prematurely sharing applicant PII with business partners/ data brokers as part of an application process would be illegal. Until then, applicants should be able to apply for a position, immediately exercise their data privacy rights (Do Not Share, delete upon rejection/ position repost/ position eliminated/ [criteria here]), and then upon on-boarding, provide their PII.

Thank you.
Michelle Smith

Begin forwarded message:

From: California Privacy Protection Agency <0000002ffddb9f13-dmarc-request@subscribe.dcalists.ca.gov>
Date: May 31, 2024 at 9:30:36 AM PDT
To: CPPA-RULEMAKING-PROCEEDINGS@subscribe.dcalists.ca.gov
Subject: CPPA to Hold Virtual Preliminary Stakeholder Session Regarding Data Broker Accessible Deletion Mechanism
Reply-To: noreply@cppa.ca.gov

News: May 31, 2024

The California Privacy Protection Agency (CPPA) invites the public to attend a virtual stakeholder session on Wednesday, June 26, 2024, from 10:00 am to 2:00 pm PDT to learn about and provide feedback on the data broker accessible deletion mechanism. The accessible deletion mechanism will allow consumers to request to delete their non-exempt personal information held by data brokers through a single request submitted to the Agency. The virtual session will include a brief presentation by CPPA staff on the accessible deletion mechanism requirements.

In addition to the online forum, the Agency also invites interested parties to submit preliminary written comments on certain requirements for the accessible deletion mechanism and other public policy considerations by 5:00 p.m. PT on Tuesday, June 25, 2024.

More information, including a copy of the invitation for preliminary comment is available here.

Please note, the CPPA has not yet introduced draft regulations on this topic, and this event is being held in advance of any formal rulemaking process. Additional public meetings will take place as part of the formal rulemaking process.

Location and Time: June 26, 2024, 10:00 AM to 2:00 PM Pacific Time (streamed via Zoom)

Register

Registration is not required but highly encouraged so we can best accommodate attendees.

About the Data Broker Accessible Deletion Mechanism

Senate Bill 362 (SB 362) tasked the Agency with creation, administration, and enforcement of the data broker accessible deletion mechanism. A data broker is defined as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. SB 362 tasks the Agency with establishing the Data Broker Delete Requests and Opt-Out Platform (DROP), which allows consumers to request from all data brokers the deletion of all non-exempt personal information related to the consumer through a single deletion request to the Agency.

About CPPA

In November 2020, California voters approved Proposition 24, also known as the California Privacy Rights Act (CPRA). The CPRA amended and expanded the California Consumer Privacy Act of 2018 (CCPA) by adding additional consumer privacy rights and obligations for businesses. It also established the California Privacy Protection Agency and tasked it with responsibilities to implement and enforce the law, including updating current regulations and implementing new ones.

Contact: databrokers@cppa.ca.gov

Read this announcement online.

From:	Jay Clark
To:	DataBrokers@CPPA
Cc:	Jay Clark
Subject:	INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING
Date:	Wednesday, June 26, 2024 1:19:42 PM
Attachments:	image001.png

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Hello,

Regarding the automated Opt-Out Database App/function. We would request that Mobile Advertising ID (MAID) be added to the input form. Our database is keyed on MAID. This will help us more efficiently process requests. Our experience has been that without the MAID, many requests are “abandoned” after multiple follow-up attempts with the data subject because we don’t receive the MAID.

Best,

Jay

Jay D. Clark
COO & Co-Founder
mobilewalla
www.mobilewalla.com

NAI
PRIVACY, TRUST & ACCOUNTABILITY

[redacted]

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. Treatment of Verifiable Consumer Requests made through the DROP
II. Privacy-protecting design of the DROP
III. Indicating the status of requests made through the DROP
IV. Consumer experience while using the DROP
V. Additional comments related to the DROP.
VI. Conclusion

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, ***<u>through a single verifiable consumer request</u>***, 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 [redacted] or David LeDuc, Vice President, Public Policy, at [redacted]

*****

Respectfully Submitted,

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

Comments from:

Aleecia M. McDonald
[redacted]
Privacy Needs Company, PBLLC

June 25, 2024

California Privacy Protection Agency (CPPA)
2101 Arena Blvd
Sacramento, CA 95834

Regarding

INVITATION FOR PRELIMINARY COMMENTS ON
PROPOSED RULEMAKING
UNDER SENATE BILL 362

<https://cppa.ca.gov/announcements/2024/20240531.html>

About the Author

Aleecia M. McDonald is the founder of Privacy Needs Company, a boutique public benefit corporation. Previously, she was the Associate Director of the Privacy Engineering program, and an Assistant Professor of the practice at the Information Networking Institute, both at Carnegie Mellon. She was the Director of Privacy at the Center for Internet and Society (CIS) at Stanford, and a Senior Privacy Researcher at Mozilla (makers of the Firefox web browser.) She co-chaired the WC3's Tracking Protection Working Group, which was an effort to establish international standards for a Do Not Track mechanism that users can enable to request enhanced privacy online. Dr. McDonald focuses on the public policy issues of Internet privacy, including user expectations for privacy tools, behavioral economics and mental models of privacy, and privacy education.

Affiliations are for identification and context only. These comments reflect the author's views alone. Thank you to hundreds of students who have shared their opt-out and delete experiences over the past years.

Summary

In this comment we urge the following courses of action:

1. Evaluate and measure all DROP proposals against the principle that **after submitting an opt-out request to a data broker, data pertaining to a Californian that originated from that data broker should no longer be collected, sold, or shared. For a delete request, such data should be deleted.**
2. Create a way for Californians to provide PII to the CPPA to provide nightly to data brokers via a **DROP List.**
3. Require a **DROP URI** in conjunction with a **DROP Dashboard** in order to allow matching of unique identifiers for pseudonymous data.
4. Require propagation of rights requests to business partners via sending null (or similar) data, including via cookie syncing platforms.
5. Request further public comments on how to realize children's privacy rights, which may require participation from different stakeholders.

Table of Contents

Introduction

Thank you for the opportunity to comment on the Data Broker Delete Requests and Opt-Out Platform (DROP) provisions of Senate Bill 362. The California Privacy Protection Agency (CPPA) has the task of designing a mechanism to afford Californians the ability to submit delete and opt-out requests en mass, to all data brokers that have registered with the state of California.

DROP is designed for scale. However, the base case for Californians exercising their delete and opt-out rights with just one data broker at a time remains a poor experience. In this comment I first explore ways to improve the user experience.

I propose the following principle as a necessary but incomplete metric:

> **After submitting an opt-out request to a data broker, data pertaining to a Californian that originated from that data broker should no longer be collected, sold, or shared. For a delete request, such data should be deleted.**

This sounds basic. However, it is not the case today due in part to several challenges outlined below. I propose that this principle be explicitly referred to when considering all DROP proposals, and that they be measured relative to how they fulfill this principle.

Typical Challenges to Delete and Opt-Out

Starting in September, 2018 just months after CCPA became law, I annually gave students the assignment to submit opt-out and delete requests and reflect upon the experience. Initially students were, understandably, unable to exercise rights that were not yet legally in force. Surprisingly, not much has improved since 2020.

Challenge 1: Asking for Personally Identifiable Data Chills Rights Requests

Major companies such as Warner Media (including cnn.com,)[1] Walmart[2], and Oracle[3] use email as an identifier to assist users with the opt-out process, not just within their own company, but as an identifier they send to third party partners. Other potential (mostly) unique identifiers include telephone number, address, and/or name.

Over several years, students independently reported PII requests as a major barrier to exercising privacy rights. Being asked to provide PII to data brokers appears to constitute a serious chilling

[1] "CNN opt-out form." WarnerMedia Privacy Center, www.warnermediaprivacy.com/do-not-sell/request/. Accessed 28 October 2020.

[2] "Walmart opt-out inquiry form." Walmart, cpa-ui.walmart.com/affirmation. Accessed 28 October 2020.

[3] "Oracle opt-out inquiry form." Oracle, www.oracle.com/legal/data-privacy-inquiry-form.html. Accessed 28 October 2020.

effect. One reason for this may be that people think since they do not know the names of the data brokers, how could data brokers have the people's names? It appears to be a fraudulent request.

Recommendations:

We recommend the CPPA create a centralized **DROP List** similar to the FTC's "Do Not Call" list. The **DROP List** would contain non-technical identifiers (such as email address, phone number, mailing address, and name,) for those who choose to provide them, along with notations for those protected as children who already have privacy rights without needing to opt-out.

The **DROP List** can be provided a batch file of all rights requests. It should be encrypted and available programmatically (that is, if companies must log into a site, that should be a step that can be automated.) It may make sense to create an entire file that grows over time, plus one that is just nightly updates.

This **DROP List** should be an optional addition to other measures listed below, with a clear explanation to Californians of how it can help facilitate rights requests (e.g. applies cross-platform and cross-browser) as well as what it does not address (e.g. pseudonymous data.)

Challenge 2: Identification and Pseudonymous Data

A great deal of user data is held pseudonymously. Technical identifiers like cookies and browser fingerprints allow the same user to be uniquely identified over time. However, there may be no PII attached to even very rich, detailed, and marketable datasets. This means that asking users for PII for identification is bound to fail.

Students regularly experienced the frustration of finding a third-party data broker's website, requesting opt-out or deletion, providing new PII, and being told there was no data associated with that PII. And yet, the data broker could go right on selling their data on the basis of unique identifiers. When companies can identify users well enough to sell their data, but not to delete it, this is a strong violation of the opening principle.

Recommendations:

1. We recommend the CPPA require all covered companies that hold pseudonymous data create a new webpage in a standard location, known as the **DROP URI**. For example, this could be something like

   http://www.example-domain.com/**.well-known/california-drop**

   The .well-known subdirectory is used by many IETF standards and is both familiar and easily implemented for companies. They can readily parse information from web server logs to read the HTTP cookies of users who visited the page. Other unique identifiers are also managed in the same way they currently identify users.

2. We recommend the CPPA add two additional fields to the data broker registration process to collect both the DROP URI as above, plus a user-facing name for the data broker.

3. We recommend the CPPA create a **DROP Dashboard** for Californians to opt-out or delete data.

A. The dashboard will allow a single button "all" option, or allow users to select which data brokers they wish to send a rights request by showing the user-facing name as provided by the data broker.

B. The dashboard will show progression through rights requests to all of the registered data brokers, and will give users an up-front estimate of how long the process may take.

C. The dashboard will manage loading the DROP URI for each data broker. Depending on the details of the user's web browser, this might be a series of redirects or opening/closing a tab for each data broker.

D. Prior to launching, the CPPA will perform or commission usability studies to ensure typical Californians understand and can use the DROP URI, with attention to multi-lingual and accessibility issues.

E. The CPPA will perform or commission a technical test at least monthly with major web browsers to ensure the dashboard continues to work, and will allocate resources to contact data brokers who have misconfigured or omitted their DROP URI.

F. The dashboard should remind Californians that it is scoped per-browser in most cases, and that they should repeat this procedure on each browser on each device.

Challenge 3: Concerns Around Fraud

During the W3C working group discussions about Do Not Track, I raised the question of fraudulent opt-outs. "MySpace is going to rise again by sending fake DNT requests for all of Facebook's users," I said facetiously. To the best of my knowledge, there are no documented cases of anything along these lines of this joke in reality. However, the Internet is known for mischief at best, and thinking about security during the design phase of a project is always a good practice.

Recommendations:
The **DROP Dashboard** uses the same technical security that companies use when they collect and sell user data. Presumably security that is good enough for collecting Californian's data is good enough for collecting their opt-outs and delete requests, considering Californians have a Constitutional right to privacy. Any measures that data brokers take to improve security during data collection will also be reflected in their security for the **DROP Dashboard**.

One interesting wrinkle is that students told me they regularly provide slightly incorrect names (e.g. change their middle initials, etc.) or have multiple email address (e.g. a series of Duck address, one per vendor) to manage fraud and spam. Companies should allow users to delete and opt-out, yet their true PII might not match government issued ID. This is another argument against requiring ID, in addition to how many Californians do not have ID — particularly children.

That said, there may be other security measures available. Provided they do not introduce new chilling effects (e.g. requiring a state-issued ID) the CPPA should welcome them.

Challenge 4: Rights Propagation and Global Competitiveness

Californians would like their opt-outs and delete requests to work for all data brokers, universally. This is what the DROP provisions are intended to address. However, not all companies outside of the United States uphold California law. This also puts domestic companies at a potential competitive disadvantage.

Recommendations:
The CPPA should require all DROP requests propagate to all business partners to the extent possible. This includes via cookie syncing platforms. Rather than requiring a new architecture for ad-tech platforms, the CPPA should require their covered companies send an update to their partners with null data to effectively "zero out" held data for each Californian who exercises a rights request.

This approach is borrowed from Google's approach to opt-outs. In their PREFID cookies, they replaced unique identifiers with the common phrase OPTOUT. It worked well, quickly, and with minimal disruption of existing systems.

Challenge 5: Children's Rights

Children do not need to opt-out under California law. Their default is opt-in. However, proposals regularly ignore this legal requirement, as do most data brokers. This violates the letter and spirit of the law.

Recommendations:
At minimum, the CPPA should allow parental- and child-originated requests, both, for the applicable age groups. This is not a very satisfying answer.

The CPPA should call for comments around realizing children's privacy rights in practice. Doing so may require more stakeholders than just data brokers.

Conclusions

As rights requests are handled today, a typical user story involves visiting a data broker website, providing new PII, being told no data match that PII so nothing is affected, only to continue to have their data collected and sold on the basis of invisible technical identifiers.

As a result, my students told me over multiple years that CPRA requests can feel like a farce or a fraud. The effect is a series of secret databases, where the entire ecosystem operates as a dark pattern. Our *status quo* violates FIPPs, violates the aims of CPRA and the DROP provisions, and violates the proposed principle offered at the start of this comment. With a system justified on the basis of consent, a Californian's "no" must not mean a data broker's "don't know" only when it is profitable and convenient.

Californians enjoy Constitutional rights to privacy. We propose ways to enact those in practice with a **DROP URI, DROP List**, and **DROP Dashboard.** In all cases, we encourage usability testing prior to deployment. Last, because technology changes (particularly around the fate of tracking cookies,) the CPPA should consider regular testing and plan to need to rework tools over time.

Thank you for the opportunity to comment.

From: Craig Erickson
To: DataBrokers@CPPA
Subject: Preliminary Comment DROP 06-24
Date: Monday, June 24, 2024 9:17:26 AM

My Public Comment to the CPPA on Accessible Delete Mechanism

As a California Consumer, I support adopting the IAB Tech Lab's Data Deletion Request Framework because:

Most registered data brokers are in the adTech industry which has no fewer than 6 professional industry associations for promoting interoperability and privacy standards among its members. It is crucial that an Accessible Delete Mechanism, used primarily by adTech firms and their advertisers at the direction of individual consumers and under the oversight of the CPPA, is fully functional on Day One, and I believe that IAB is best positioned to disseminate and expedite this tool within the adTech Ecosystem.

Many non-registered data brokers are also in the adTech industry or used by the adTech industry, and they can be incentivized to register when they gain access to the Data Deletion Request Framework. This facilitates downstream cascading delete and opt out requests for data brokers and for advertisers who act on behalf of their customers' privacy preferences, and could provide a directory service that is scalable and easier to maintain through the API recommended by the IAB Tech Lab than the current Data Broker Registry webpage hosted by the CPPA. One challenging task for all stakeholders is maintaining entity status of parent companies and their subsidiaries, as well as data brokers that operate across multiple domains.

The CPPA should not build its own accessible delete mechanism, contract it out to a third-party, or host and operate the Site or Tool because it is outside of the CPPA's core competency and there are potential conflicts between an enforcement role vs. an administrative or customer service role.

The Data Deletion Request Framework can also be extended to other rights requests. The same parameters used to conduct searches for deletion can be reused for know, correct, and limit requests. The same schema used to specify custom identifiers can be reused to specify custom rights requests, similar to the Digital Rights Protocol proposed by Consumer Reports, to maximize standardization of rights requests while supporting flexibility of options.

In closing, the best reason for adopting IAB Tech Lab's Data Deletion

Request Framework is to broaden the scope and capabilities of advertisers, consumers, employers, data brokers, authorized agents, etc. across all jurisdictions to use the tool for complying with the CCPA and other privacy laws.

Sincerely,

Craig Erickson, a California Consumer

From: Kale Smith
To: DataBrokers@CPPA
Subject: Comments for SB 362: Accessible Deletion Mechanism
Date: Tuesday, June 25, 2024 10:19:06 PM

This Message Is From an External Sender
WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Hello,

As a primary contributor to the IAB Tech Lab's Data Deletion Request Framework (DDRF), I wanted to provide relevant information regarding the design of the framework that could help inform the accessible deletion mechanism for SB 362.

I would like to first preface that the recently finalized DDRF was developed in part to provide a protocol to comply with CPRA requirements for communicating deletion requests from a first party to third parties. Despite initial scope limitations, the framework was intended to be extensible to future needs and I believe could be adapted to support SB 362 with few modifications.

1. **Deletion vs. Opt-out**
   a. 1798.99.86 (d)(1) requires a data broker to delete a consumer's personal information "at least once every 45 days", and 1798.99.86 (d)(2) requires a data broker to "not sell or share new personal information" of the same consumer.
   b. Given that data deletion and sale/share opt-outs can follow different processes within an organization, there may be a repeating 45-day window in which a data broker could potentially ingest/repopulate previously deleted personal data (e.g. a birthdate) that the broker may not have considered "new" personal information as it comes from pre-existing business processes. If a data broker ingests data weekly and sells/shares data monthly, this could lead to a user's data inadvertently being shared in between each 45-day data deletion if the opt-out is not clearly applied to previously deleted personal information as well.
   c. The DDRF was ostensibly built to communicate a data deletion of personal information, not an opt-out of a data sale/share, so its use could potentially be interpreted to only oblige a data broker to perform a data deletion and not a subsequent opt-out of data sale/share for the same data of a given consumer. There is no technical reason in the framework to prevent data brokers from taking both actions, and this requirement could be made clear with policy guidance.
2. **Push vs. Pull**
   a. 1798.99.86 (c)(1) requires data brokers to "access the accessible deletion mechanism […] at least once every 45 days".
   b. The DDRF was designed to be processed via real-time APIs (i.e. a push action)

in order to meet data deletion timeline requirements. However, there is no technical reason that the APIs could not be sent upon broker request (e.g. a pull action). The DDRF ensures that each deletion request is unique to a single user ID, originating first party, and timestamp. This was chosen to maintain data provenance and to assist in troubleshooting of an individual deletion request, if necessary.

   c. The DDRF could potentially be extended to support batch communication of user requests, though this would potentially require reworking of the signing/encryption logic to ensure validity of the request(s).

3. **Receipt Acknowledgement**
   a. 1798.99.86 (e)(1) enables a third party to audit the compliance with the deletion mechanism every three years.
   b. 1798.99.86 (c)(1)(B) acknowledges that data brokers may deny a consumer request to delete “because the request cannot be verified”.
   c. The DDRF requires receipt acknowledgement to enable auditing between parties as well as close the communication between two parties handling a deletion request. This is necessary in case a request must be resent due to being lost in transit or invalid parameters were used. Currently there is a status code for successful receipt, as well as various failure codes that a request is unable to be processed from a technical standpoint (e.g. a malformed request). There is no status code for actions taken after request receipt. This was purposely chosen to prevent the DDRF from proactively exposing consumer information (e.g. the existence of a user ID in a database), as well as to encourage immediate feedback in case a request must be resubmitted.
   d. There is currently no receipt status code in the DDRF representing a denial of processing for policy reasons (e.g. information is exempted from deletion), although the framework could be extended to support such use cases as needed. The DDRF does not currently define a timeframe for responding to a request with a receipt acknowledgement, nor does it define behavior if multiple receipts for the same request are received (i.e. asynchronous receipts are possible).

4. **Security and User Identification**
   a. 1798.99.86 (a)(1) requires “reasonable security procedures and practices” to “protect consumers’ personal information from unauthorized use, disclosure”.
   b. The DDRF was designed to mitigate against potential malicious actors present in the ecosystem. The security provided by the protocol is maintained via industry-standard use of JSON Web Tokens (JWTs) that ensure the contents of a request have not been modified in transit. This protects against spoofing and replay attacks. JWTs have a well-established method for cryptographic key management.
   c. The DDRF places implicit trust in the originating first party that generates a deletion request on behalf of the consumer to have verified the consumer’s identity. Once verified, the chosen ID that is communicated to downstream recipients is purposely undefined by the DDRF to allow each business to determine their preferred ID format. Hashed emails are expected to be a common ID format to mitigate user exposure and is supported by the DDRF. Encrypted ID formats are not explicitly supported by the DDRF, but it is expected that DDRF requests would be encrypted in transit (via HTTPS).

Best,

Kale Smith
Sr. Product Manager - Privacy
[redacted]
Roku

From: Sylwia Januszewska
To: DataBrokers@CPPA
Cc: [redacted]
Subject: Preliminary Comment DROP 06-24
Date: Wednesday, June 26, 2024 3:21:15 AM

This Message Is From an Untrusted Sender
Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Dear CPPA Board,

Roqad, as a data broker, would like to provide comments on the topics raised within:
https://cppa.ca.gov/regulations/pdf/invitation_for_comments_drop.pdf

1. Verifiable consumer requests
We suggest that DROP (Data Broker Delete Requests and Opt-Out Platform) has a validation mechanism implemented that verifies the request based on official data also managed by CPPA. This applies either to the user making the request directly, or to the intermediary acting on their behalf (legitimising the POA).

For example - registering the end-user (requester) at the initial submission phase, by checking his uniquely identifying data on the platform, could enable the confirmation of the requester.

2. Privacy protection
We suggest implementing appropriate privacy and security settings on DROP (in particular an encrypted communication channel) to protect the privacy of the information provided.
Data brokers could have direct access to the list of requests provided through the platform with appropriate security and encryption settings. An API should also be available on the platform, for integration with the data broker's internal opt-out solutions. In addition, one may be tempted to prepare a DROP API to connect to existing request handling systems on the market (Jira Service Management, Freshdesk, Zendesk, Servicenow, etc.) used internally by multiple entities.

The DROP API or its specification should be ready a few months before 1 August 2026 to allow enough time for integration.

3. Request status
It is likely that the number of data deletion requests may be high, so providing a DROP API may reduce the effort spent on managing the requests. A DROP API to connect to an internal opt-out solution may allow information to be shared that a particular data broker has confirmed that the request is valid (there was a requester entry in the database) or not, and to provide information on the status of the request, if applicable.

In case of any further questions, do not hesitate to contact us.

Best regards,

Sylwia Januszewska

Roqad / Head of Privacy and Security

[redacted]

WORLD **PRIVACY** FORUM

Comments of World Privacy Forum to California Privacy Protection Agency Board regarding Preliminary Comment DROP 06-24

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

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

26 June 2024

Thank you for the opportunity to provide feedback regarding CPPA's invitation for preliminary comments on proposed rulemaking under Senate Bill 362. In these comments we are providing some followup and feedback to the legal team regarding the Delete Act implementation. In particular, we are providing resources that the legal team may want to consider in regards to the Delete Act implementation.

I. Financial Industry Regulatory Authority (FINRA)

FINRA is a U.S. non-profit organization that oversees the integrity of securities markets. https://www.finra.org/about They are unique in structure; they are one of the only NGOs authorized by Congress to act as a financial sector regulatory authority alongside the Securities and Exchange Commission.

Of interest for California, FINRA uses a robust, real-time AI-based system to monitor the securities markets, tracking all brokers. A tool called FINRA BrokerCheck https://brokercheck.finra.org is worth examining for ideas regarding the data broker registry. One idea is that legitimate data brokers who register in California could have basic background information made available to the public to support the opt out feature.

Of overall interest is FINRA's RegTech knowledge, which they now share via conferences, written materials, etc. https://www.finra.org/media-center/finra-hosts-first-regtech-conference

I would encourage California to discuss with FINRA what models you might be able to borrow or learn from.

II. Consumer Financial Protection Bureau (CFPB)

The CFPB https://www.consumerfinance.gov was created during the 2008 U.S. financial crisis. It overseas the large financial sector actors, such as banks and consumer reporting agencies. It also has authority over the databroker sector via the various Fair Credit Reporting Act structures, and it has put forward significant work in this area. We encourage you to talk with the CFPB leadership to hear how you may integrate with their work.

Some key resources:

- *Comments of CFPB Director Chopra at White House Roundtable on Data Brokers (2023*): https://www.consumerfinance.gov/about-us/newsroom/remarks-of-cfpb-director-rohit-chopra-at-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/

- *CFPB Inquiry into the business practices of data brokers*: https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-into-the-business-practices-of-data-brokers/ CFPB published an RFI regarding data brokers. It was preparatory work that is informing the planned rulemaking of databrokers under the FCRA.

- *WPF Data Broker Comments to CFPB*: WPF submitted extensive comments regarding the Data Broker RFI, which we have included in these comments. The full comments, as filed, may be found in Appendix A. Here, we note two items. First, data brokers may own or have a variety of business partnerships with identity resolution companies. This creates meaningful complications regarding opt-out mechanisms that are verifying consumer identity. Second, opt out in general has become less effective due to the impacts of advanced AI and deep machine learning. Quoting from our comments:

  > "….if there is just one thing these comments could impress, it would be that to solve the problems of data brokers today the problems must be seen as a system, and the solutions must be seen as part of a system. The understanding needs to also encompass the total ecosystem of data, technology, and AI-fueled analysis that wraps around these varying systems. Today's data ecosystems and associated analytical systems are stunningly advanced, facilitating analysis of even data that has been de-identified. How does opt-out work on de-identified data? It does not." (Full comments in Appendix A.)

This idea of opt out of single consumers from single data broker systems or companies is greatly complicated by the reality "on the ground" regarding just how difficult individual opt outs have become. A core problem the CPPA will need to solve is what to do when consumer information has been aggregated to varying degrees and an opt out is still desired.

III. AAMVA Mobile Driver License (mDL)

AAMVA is leading the mDL efforts in Northern America, with specific efforts inclusive of the U.S. and Canada. California is involved in a large mDL pilot implementation. We encourage the CCPA to meet with the AAMVA regarding the mobile driver ID or mDL, as it is highly relevant to current and future identity issues including data broker opt out. The AAMVA has many resources of interest. https://www.aamva.org/topics/mobile-driver-license#?wst=d5a5f5751f7474b62a5bb2b374692b61

IV. Conclusion

In considering how best to implement data broker opt-out in California, will be important for the CPPA to understand the deeper ecosystems that data brokers work in, including identity ecosystems, and effectuate the opt-out with privacy protections and appropriate data minimization while still facilitating correct identity verification.

Thank you again for your work. We stand ready to assist with any information or research that would be supportive of your efforts.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum

Appendix A: Copy of comments made by the World Privacy Forum to the CFPB regarding its Data Broker RFI, filed under Docket No. CFPB-2023-0020 on 15 July 2023.

Comments of the World Privacy Forum to the Consumer Financial Protection Bureau regarding Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, Docket No. CFPB-2023-0020

Sent via [redacted] *with cc: to* [redacted]

Erie Meyer, Chief Technologist and Senior Advisor, Office of the Director
Davida Farrar, Counsel, Office of Consumer Populations
Request for Information Regarding Data Brokers
Consumer Financial Protection Bureau
[redacted]

15 July 2023

The World Privacy Forum is pleased to provide comments regarding the Consumer Financial Protection Bureau's *Request For Information (RFI) regarding Data Brokers,* 88 FR 16951, https://www.federalregister.gov/documents/2023/06/13/2023-12550/request-for-information-regarding-data-brokers-and-other-business-practices-involving-the-collection . The World Privacy Forum (WPF) is a nonprofit, non-partisan 501(c)(3) public interest research group.[1] WPF focuses on multiple aspects of privacy, with governance of complex data ecosystems being among our key areas of work (technical, legal, and policy). We have conducted and published extensive research for 20 years and counting, including original peer-reviewed data

[1] World Privacy Forum, https://www.worldprivacyforum.org

and technology governance research published at the highest levels,[2] among collaborative multi stakeholder work at the multilateral level.

Specific to the RFI regarding data brokers, WPF has conducted extensive past and current research and work specific to data brokers and data broker ecosystems. Our reports about data brokers include *The Scoring of America: How secret consumer scores threaten your privacy and your future,*[3] which was the first predictive analytics report analyzing data broker activity in regards to Artificial Intelligence and machine learning. *The Scoring of America* was cited by the Obama White House in its White House Big Data report[4] as well as by the FTC report on data brokers. Another WPF report, *Data Brokers and the Federal Government*,[5] led to positive change in practices regarding certain consumer practices. We have testified regarding data brokers before Congress four times, each time submitting substantive written testimony, and we testified and participated in the Vermont educational hearings process regarding data brokers which led to the nation's first data broker registry. WPF has additional substantive expertise in identity ecosystems, and WPF's executive director was named one of the leading global digital identity experts in 2021. Digital ID and data broker ecosystems are intertwined, something that has not been well-documented in the US Federal work on data brokers.

Beyond our own research and work, WPF co-chairs the data governance working group in the UN Statistical Commission's Global Task force, and participates in the World Health Organization as co-chair of the Research and Academia Network Constituency, and serves on a separate WHO data governance workgroup. WPF participated in the OECD's AI Network of Experts during the drafting of the OECD Recommendations on Artificial Intelligence and currently participates in the AIGO Working Party in three expert working groups, including the AI Foresight Group. You can find out more about WPF's work and see our reports, data visualizations, testimony, consumer guides, and comments at http://www.worldprivacyforum.org.

The CFPB RFI regarding data brokers is broad, and requests information about a broad array of topics in the data broker ecosystem. In considering what would be most useful, these comments outline, describe, analyze, and document the data broker activities at an ecosystem level regarding technical, legal, and policy components of the ecosystem, and what approaches could help mitigate the problems in the ecosystem. Much of the work being done today regarding data brokers does not encompass the ecosystem level structure and dynamics of the issue, and

[2] *A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.* Pam Dixon, Springer Nature, Health Technology. DOI 10.1007/s12553-017-0202-6. http://rdcu.be/tsWv. Open Access via Harvard-Based Technology Science: https://techscience.org/a/2017082901/.

[3] Pam Dixon and Robert Gellman, *The Scoring of America: How secret consumer scores threaten your privacy and your future*, World Privacy Forum, 2014. https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/ .

[4] *Big Data, Seizing Opportunities, Preserving Values*, Executive Office of the President of the United States (White House Big Data Report).

[5] Robert Gellman and Pam Dixon, *Data Brokers and the Federal Government: A new front i the battle for privacy opens*, 30 October 2013. https://www.worldprivacyforum.org/2013/10/report-data-brokers-and-the-federal-government-a-new-front-in-the-battle-for-privacy-opens/ .

WPF has concerns that this will lead to piecemeal approaches that do not tackle the root challenges. WPF also has concerns that the data broker ecosystem is either at or in the process of passing through a watershed point beyond which mitigations will become less and less possible.

The conversation about data brokers in the US context does not appear to be fully aware of the past, nor even the present state of data broker ecosystems; and it is no wonder; the data broker ecosystem is stunningly complex. These comments attempt, with as much brevity as possible, a snapshot of this ecosystem and its evolution, concluding with how the risks this ecosystem poses might be mitigated.

To begin, these comments examine the exponential curve of the data broker ecosystem by comparing where data brokering was in the late 1980s and early 1990s to where it is today. There is very little documentation of the early data brokering ecosystem anymore, however, WPF has gathered key aspects of this data and presents it in these comments in brief. These comments also discuss the relationship of the Fair Credit Reporting Act to the data broker ecosystem. And finally, these comments briefly touch on the role of digital identity in the data broker ecosystem, a neglected aspect of regulation that needs attention. Taken together, the comments will provide a landscape view of the data broker ecosystem, at technical and policy levels, which is essential to understanding how to proceed forward toward mitigations and solutions.

I. Introduction

The modern privacy and governance challenges that data brokers pose to the American public are profound, and they operate in the rarified air of growth curves that are among the most difficult for human brains to process; that is, exponential curves. These are the kinds of curves that have befuddled even the smartest, most well-educated people, and have caused many to underestimate materially important matters such as the speed of climate change, how debt to income ratios work, and today, how data brokers are operating in today's complex and entangled data ecosystems in ways that affect everything from business processes to peoples' and groups of peoples' lives. Data brokers are not operating on a linear curve. They are operating on an exponential curve, and this has consequences for policy and for people.

Willis Ware, the computer scientist who famously worked with John von Neumann building an early computer at Princeton in the late 1940s to early 1950s, is credited with creating the field of computer security in 1970 with his landmark publication, *The Ware Report*. [6] Ware understood exponential curves, he understood computer ecosystems, and he understood privacy. Thanks to these gifts, he saw around a lot of corners. He wrote in the late 1960s: "The computer will touch men everywhere and in every way, almost on a minute-to-minute basis." He penned these

[6] The 1967 Spring joint Computer Conference session organized by Willis Ware and the 1970 *Ware Report* are widely held by computer security practitioners and historians to have defined the field's origin. See: IEEE Annals of the History of Computing https://dl.acm.org/doi/10.1109/MAHC.2016.48 Willis H. Ware Papers , CBI 40, http://purl.umn.edu/41431; See also W.H. Ware, RAND and the Information Evolution: A History in Essays and Vignettes, RAND, 2008; www.rand.org/pubs/corporate_pubs/CP537.html .

words just before he chaired the the famous U.S. hearings [7] that provided the evidentiary basis for the "HEW Report," shorthand for a bedrock report on privacy which stated in full is *Records, Computers and the Rights of Citizens: Report of the HEW Advisory Committee on Automate Personal Data Systems*,[8] which in turn first articulated the Fair Information Practices, or FIPs.

At the time, there was a great deal of concern about the Social Security Number and its potential for abuse, and generally about the "automation of personal data record keeping operations" by the US government. Ware looked at the emerging world of networked computers, databases, unique personal identifiers like the SSN, and third party data use and saw specific risks which he and others at the time worked collaboratively to mitigate.

FIPS became a bedrock for early privacy law; the European Data Privacy Directive, EU 95/46, is in large part dependent on Ware's initial collaborative work on developing the Fair Information Practice principles (FIPS).[9] EU 95/46 was grounded in FIPs, something Ware was proud of.[10] This early EU data privacy law went on to form the backbone of the modernized General Data Protection Regulation (GDPR) in 2018. FIPs is also the structure upon which HIPAA in the US rests, among other privacy laws in the US and around the world. [11]

The data ecosystems Ware saw as being subject to exponential curves in his time have indeed proven to be exactly that; the ecosystems have grown in scope and complexity as he expected, and steep section of the exponential curves are becoming apparent.

Ware was among the first scientists to fully articulate computer and data risks beginning in the late 60s. These comments begin with Willis Ware because today, it will be necessary to think like Ware, but for our time, to see where we are now and to work to anticipate and mitigate what comes next. US policy makers have failed to reign in data broker activities, even when there is clear evidence of harms to people and groups of people resulting from data broker activities. We can and we must do better, or risk being locked into an unhealthy ecosystem. Data broker lock-in is a real possibility at this point, which these comments will explain.

[7] Hoofnagle, Chris Jay, *The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS).* Archival text uploaded July 15, 2014. https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/archive-of-the-meetings-of-the-secretarys-advisory-committee-on-automated-personal-data-systems-sacapds/

[8] *Records, Computers and the Rights of Citizens: Report of the HEW Advisory Committee on Automate Personal Data Systems*, DHEW Publication No. (OS) 73-94 (July 1973). https://www.justice.gov/opcl/docs/rec-com-rights.pdf

[9] Robert Gellman, *Fair Information Practices: A Basic History.* http://bobgellman.com/rg-docs/rg-FIPShistory.pdf. A brief introduction is here http:/www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

[10] *An Interview with Willis H. Ware, Oral History 356*, Conducted by Jeffrey R. Yost on 11 Auugust 2003, Santa Monica, California. University of Minnesota. https://conservancy.umn.edu/bitstream/handle/11299/107703/oh356ww.pdf .

[11] A current discussion among privacy and AI ethicists is if FIPs is enough for the changed AI -driven ecosystems. An early consensus is forming that the FIPs will not be sufficient, and will need be transmuted and built upon to adapt to the changes.

The evidentiary hearings that led to the enactment of the Fair Credit Reporting Act curtailed certain abuses of credit reporting in the United States at that time. These discussions were part of a first, early push in US privacy regulations, which also generally included in the US the Privacy Act and the Family Educational Rights and Privacy Act (FERPA). It is becoming more apparent that the US has reached a point where something similar will need to occur for a changed data era.

II. Data broker ecosystems

Data brokers are not a shiny new topic. There have been extraordinary reports about data brokers and harms resulting from data brokers. Here, these comments begin with a seminal report by Chris Jay Hoofnagle, now a Berkeley Law Professor, who in 2003 published *Big Brother's Little Helpers.* This report stands as the first major modern reporting of data broker activities.[12] In this report, Professor Hoofnagle documents the myriad ways that the US government relies on data collected by third parties, data that has levels of accuracy that are non-transparent and questionable.

Surprised at the time that there was not a regulatory response to Professor Hoofnagle's report, WPF followed on Hoofnagle's work with a 2013 report, *Data Brokers and the Federal Government.* This report analyzed the data broker purchasing activities of the Federal Government in light of the then-new OMB guidance regarding its Do Not Pay policy. The Treasury's implementation of the "Do Not Pay" portal included information from a commercial database called the Work Number, a database that was not a government-held database and was not subject to the Privacy Act. The WPF report concluded:

> The government must bring itself fully to heel in the area of privacy. If it is going to outsource its data needs to commercial data brokers, it needs to attach the privacy standards it would have been held to if it had collected the data itself. Outsourcing is not an excuse for evading privacy obligations.
>
> This report discusses new Office of Management and Budget (OMB) guidance for an initiative (Do Not Pay Initiative)[13] that on one hand provides for expanded use of commercial data brokers by federal agencies and on the other it establishes new privacy standards for the databases used in the Initiative. Although incomplete, its extension of privacy standards to commercial databases purchased by the federal government is groundbreaking. As such, this report recommends that OMB should expand its new guidance to cover all government data purchases, bartering, and exchanges from commercial data brokers and databases containing personal information. The problems created by unregulated government use of commercial data sources need to be seen clearly and addressed directly.

[12] Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and other commercial data brokers collect and package your data for law enforcement*, EPIC, 2003. https://lawcat.berkeley.edu/record/1118906

[13] OMB Memorandum M-12-11, Reducing Improper Payments through the "Do Not Pay List" (Apr. 12, 2012), available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12- 11_1.pdf.

> If all federal government uses of commercial data brokers are not required to satisfy the new OMB guidelines at a minimum, then the very databases that are supposed to be used for society's benefit will be less accurate, timely, relevant, and complete, and can therefore cause unnecessary and avoidable harms such as garbled identities, blocking individuals from government benefits, and potential misclassification or even law enforcement actions against people due to errors in data. On a broader level, a lack of trust in the government's ability to properly protect fair information rights in a new digital era can be the expensive societal result."

Although Professor Hoofnagle wrote his report now 20 years ago, and although WPF published its report regarding government use of commercial data 10 years ago, the lessons articulated to the US government have yet to be digested and acted upon. In 2023, the Office of the Director of National Intelligence (ODNI) released and declassified a report discussing problems with the US use of commercial data brokers.[14] While this action was the right thing to do, it inadvertently documented the practices that are as of yet still not constrained by appropriate guardrails.

The ODNI report is helpful in several respects in determining the contours of the modern data broker ecosystem. The report, *The Office of the Director on National Intelligence Senior Advisory Group Panel on Commercially Available Information*, approved for release 5 June 2023, documents that the US government intelligence community purchased commercial available information, which is described in the report as clearly providing intelligence value. The ODNI report states that commercially available information:

> "…clearly provides intelligence value, whether considered in isolation and/or in combination with other information, and whether reviewed by humans and/or by machines. It also raises significant issues related to privacy and civil liberties. The widespread availability of CAI regarding the activities of large numbers of individuals is a relatively new, rapidly growing, and increasingly significant part of the information environment in which the IC must function."

This is a clear indication that data brokers' practices of selling data about consumers to the Federal government is not going to be stopping any time soon, not if national security interests in the US are finding that data useful. It is helpful that the ODNI markedly stated that they saw the data brokering raises significant issues relating to privacy and civil liberties, however, while the World Privacy Forum agrees with the ODNI that data broker activities are a rapidly growing and increasingly significant part of the information environment, it cannot be reiterated too many times that data brokering activities are operating on an exponential curve, where activities are doubling. This means that data brokering will get much, much more prevalent much more quickly than policy makers may realize. Because growth of this type is very difficult to manage as it reaches the upper curves, which is where data brokering is heading now, it is no longer enough to simply state what has been documented for 20 years now: that collection and sale of commercially available information about consumers in ODNI's words, "raises significant issues related to privacy and civil liberties."

[14] *The Office of the Director on National Intelligence Senior Advisory Group Panel on Commercially Available Information*, approved for release 5 June 2023. https://www.odni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf .

WPF's analysis is that government use of data broker data, by ODNI and other national security and law enforcement entities, will require a different set of guardrails than CFPB is considering. For this reason, in these comments we set aside the discussion of this aspect of the data broker ecosystem in these comments save for mentioning one last item: which is that government purchase of data broker data in general provides substantive baseline funding for the data broker ecosystem as a whole. Without government support of data broker activities, the economic fundamentals of the data broker industry would be much weaker. Beyond law enforcement and national security purchases of data broker data, which deserve extensive fresh discussions, so too does purchases of consumer data from data brokers by other Federal agencies.

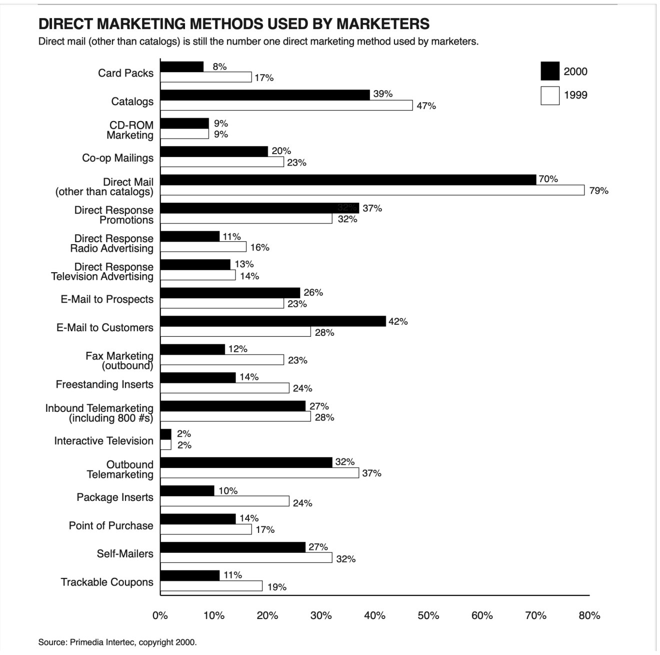
The following overview of data broker ecosystems now turns to a bird's eye view of data broker chronology to show in more detail the longitudinal growth aspect of the data broker ecosystem.

A. Data Broker Ecosystems: The past

Initial data broker ecosystems looked quite different before the Internet. These activities can be largely characterized as direct marketing, data cleaning, and support activities, such as printing and mailing envelopes. Lists of people and their details and preferences were sold via large paper books filled with data cards printed on paper.

These books used to be available in paper formats and were heavy, thick books. As time went on, these same data cards and marketing lists were digitalized, and became databases. Later still, the lists were offered via real-time or near real time APIs.

The data broker ecosystem can be plainly seen in the statistical recording of its activities at the time. Card packs, freestanding inserts, and other paper-based marketing were still in use, but even just from 1999 to 2000, their use was dropping.



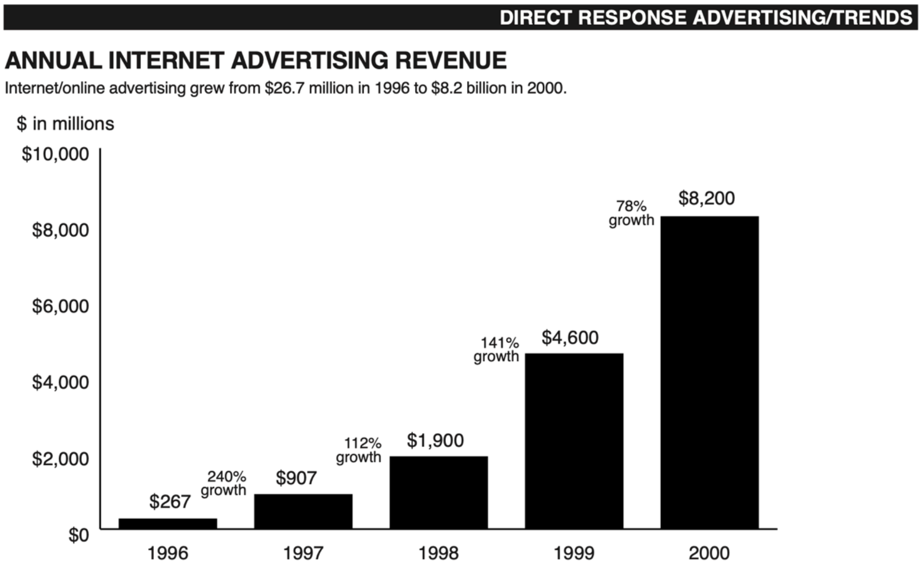
DIRECT MARKETING METHODS USED BY MARKETERS

Direct mail (other than catalogs) is still the number one direct marketing method used by marketers.

Source: Primedia Intertec, copyright 2000.

Source: The 2001 DMA Statistical Factbook, Archival copy via University of Washington. Available at: http://courses.washington.edu/dmarket/2001Factbook.pdf . Page 25.

In the same 2001 DMA volume, annual Internet advertising revenues increased from $26.7 million in 1996 to $8.2 billion in 2000. The growth curve is unambiguous, which tells the story of the late 1990's to early 2000's and the impact of the then relatively young Internet.



DIRECT RESPONSE ADVERTISING/TRENDS

ANNUAL INTERNET ADVERTISING REVENUE

Internet/online advertising grew from $26.7 million in 1996 to $8.2 billion in 2000.

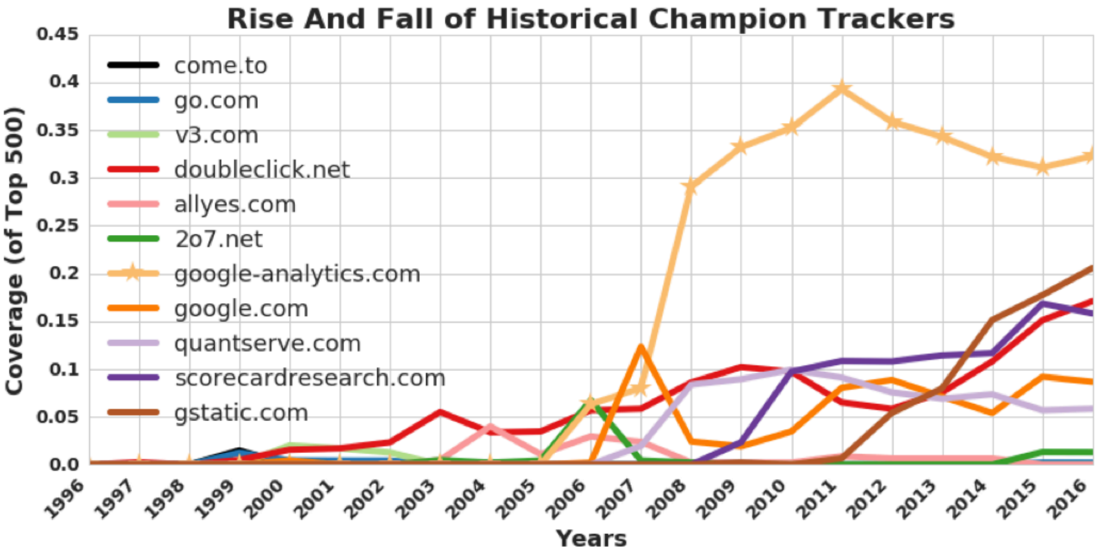
Source: Statistical Fact Book 23rd Edition, Direct Marketing Association, 2001. Archival copy available at University of Washington: http://courses.washington.edu/dmarket/2001Factbook.pdf . Page 29, Annual Internet advertising revenue from 1996 - 2000.

In 2016, a team from the University of Washington published a remarkable study of web tracking from 1996 to 2016.[15] This is an important study, because academic study of web tracking only began in 2005. The UW study utilized a complex technical process to document and fill in the gaps in knowledge for tracking prior to 2005.

[15] Ada Lerner, Anna Kornfeld Simpson, Tadayoshi Kohno, and Franziska Roesner, *Internet Jones and the Raiders of the Lost Trackers: An archaeological study of web tracking from 1996 to 2016,* University of Washington. Proceedings of the 25th USENIX Security Symposium, August 10-12, 2016. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/lerner .

Notably, this work documented that in 2016, 90% of the 500 top websites sent information about their visitors to at least one third party.

Here, one of the many data visualizations in the paper shows the rise and fall of historical champion trackers for the top 500 websites. The graph shows the outcomes are comprised of a variety of “tracking curves.” Most curves begin flat in 1996, as the web was just developing, then in 2007, Google-analytics.com trackers begin to demonstrate the start of an exponential curve up until 2011, when it cooled a bit. The rest of the trackers demonstrate more linear curves, which is not a surprising result.



Source: Internet Jones and the Raiders of the Lost Trackers: An archaeological study of web tracking from 1996 to 2016, University of Washington. Proceedings of the 25th USENIX Security Symposium, August 10-12, 2016. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/lerner . Page 1008.

WPF is not remarking on the advertising ecosystem per se here. The point is to demonstrate the historic shifts of tracking online, specifically, on the web. These extraordinary shifts from analog marketing tracking to web tracking correspond to the growth and digitalization of data brokering. Today, charting tracking would be more difficult, as the digitalization of the ecosystem goes far beyond the web and encompasses myriad devices, IoT, apps, and digital wallets. The broad strokes can be seen in these data: the data ecosystems of our time moved from analog to digital, and they did so fairly rapidly, with exponential curves that began in earnest in 2000, and became more obvious in less than 10 years.

In 2011, WPF testified before Congress regarding data broker harms to consumers. Skimming the testimony will quickly reveal that the general topics of discussion were far more basic at that time than today. The ecosystem was still emerging from the analog world. By 2013, WPF had spent 6 years researching modern data broker practices at that time. Our 2013 Congressional testimony was focused on what we had found. We found numerous data broker lists, which we documented in our testimony. We also discussed something new: consumer scores, and how data brokering was beginning to modernize and turn to machine learning and predictive algorithms to categorize people. This shift to the rise of machine learning in data brokering brings us to the present.

B. Data Broker Ecosystems: The Present

This section of the comments sketches some of today's characteristics of the data broker ecosystem. In a phrase, it is profoundly complex, and this has consequences for crafting legal and policy solutions.

Machine learning, not lists

As mentioned, in 2014, WPF published its *Scoring of America* report, which was 7 years in its research, and was the first report on data brokers to document and modernize the understanding of the data broker ecosystem. In this report, WPF did not focus on lists of consumers that data brokers were selling, because that practice was and still is receding. A new form of data brokering was becoming prominent, which was scoring people, and groups of people, and classifying them into categories and types of people, consumers, purchasers, etc. An era of AI and machine learning was coming, and the *Scoring of America* is a benchmark for the beginning of that era. The report forms a bridge between more analog data broker ecosystems and present-day data broker ecosystems.

The summary of the report states:

> This report highlights the unexpected problems that arise from new types of predictive consumer scoring, which this report terms consumer scoring. Largely unregulated either by the Fair Credit Reporting Act or the Equal Credit Opportunity Act, new consumer scores use thousands of pieces of information about consumers' pasts to predict how they will behave in the future. Issues of secrecy, fairness of underlying factors, use of consumer information such as race and ethnicity in predictive scores, accuracy, and the uptake in both use and ubiquity of these scores are key areas of focus.
>
> The report includes a roster of the types of consumer data used in predictive consumer scores today, as well as a roster of the consumer scores such as health risk scores, consumer prominence scores, identity and fraud scores, summarized credit statistics, among others. The report reviews the history of the credit score – which was secret for decades until legislation mandated consumer access -- and urges close examination of new consumer scores for fairness and transparency in their factors, methods, and accessibility to consumers.

Defining consumer scoring

The World Privacy Forum defines a consumer score as follows:

> A consumer score that describes an individual or sometimes a group of individuals (like a household), and predicts a consumer's behavior, habit, or predilection. Consumer scores use information about consumer characteristics, past behaviors, and other attributes in statistical models that produce a numeric score, a range of scores, or a yes/no. Consumer scores rate, rank, or segment consumers. Businesses and governments use scores to make decisions about individual consumers and groups of consumers. The consequences can range from innocuous to important. Businesses and others use consumer scores for everything from predicting fraud to predicting the health care costs of an individual to eligibility decisions to almost anything.

It is critical to understand this particular aspect of the evolution of data brokering: *data brokering is moving away from lists and databases of consumers.* It has moved toward scoring consumers in clusters, groups, households, and sometimes individually. Consumer scoring is already more widespread than most people realize. Thousands of consumer scores exist, perhaps more. How many Americans have them? Almost all do. Minors are less likely to be scored than adults, although they, too can have or influence some consumer scores. For example, household scores often reflect interests and activities of minors.

Among American adults, each individual with a credit or debit card or a bank account is likely to be the subject of one or more scores. Individuals who buy airline tickets have a score. Individuals who make non-cash purchases at large retail stores likely have a score.

Scores like the medication adherence score, the health risk score, the consumer profitability score, the job security score, collection and recovery scores, frailty scores, energy meter scores, modeled or "aggregate" credit scores, youth delinquency score, fraud scores, casino gaming propensity score, and brand name medicine propensity scores are but a few of the numbers that score, rank, describe, and predict the actions of consumers.

In short, almost every American over the age of 18 has at least one score, and most adult Americans have many scores. An individual could easily be the subject of dozens or even hundreds of secret consumer scores. We can safely predict that there will be many more consumer scores in the future. Fed by the masses of consumer data now available, consumer scoring is quickly becoming a simple shorthand to make sense of a sea of information.

How AI and consumer scoring complicates data control and opt-outs

WPF in the past promoted data broker opt-out mechanisms as a solution for consumers. The ideal of the early 2010 era was to find a way to create a "one stop opt out shop" for consumers. This ideal is no longer relevant today. AI has profoundly complicated the idea of consumers "controlling their data" or "opting out" of data broker ecosystems. The trends of the 2014 *Scoring* report have become much more pronounced and entrenched, and it has grown increasingly apparent that data broker opt out is not a realistic choice for a mitigation solution.

In January 2023 NIST published an influential management standard for AI risks, the *NIST AI Risk Management Framework.*[16] Looking at this framework, it becomes clear that opting out can no longer be considered an effective remedy or mitigation for data broker challenges: the

[16] *NIST AI Risk Management Framework and Playbook*, NIST, January 2023. https://www.nist.gov/itl/ai-risk-management-framework .

ecosystem is too complex, has too many layers, and the data is becoming more diffuse. AI and machine learning operate in systems. While much is written about algorithms, it is in reality the *system* of AI that counts, and the supporting or enveloping ecosystem.

If there is nothing else that comes from these comments, if there is just one thing these comments could impress, it would be that to solve the problems of data brokers today the problems must be seen as a system, and the solutions must be seen as part of a system. The understanding needs to also encompass the total ecosystem of data, technology, and AI-fueled analysis that wraps around these varying systems. The systems of today are stunningly advanced, facilitating analysis of even data that has been de-identified. How does opt-out work on de-identified data? It does not. Consumer data is embedded in systems that are within a larger and opaque ecosystem.

As can be seen in the NIST RMF, today's multi-layered and complex cloud data technology infrastructure combined with the AI processing and analysis that data brokers are utilizing becomes increasingly crowded and complex. The activities of protecting the security of people's data, ensuring it is accurate, and responding to opt-out requests has become increasingly challenging. It is not difficult to forecast that at some point soon, opting out will be understood to be an unworkable solution for consumers.

To give an example of why this is already a near-reality, consider how significant of a challenge it is to keep track of data after it has been replicated, split, and /or fed into algorithmic and machine learning systems. Individual's data or household or census block data might be incorporated into several different intersecting models and data sets, which are then crunched into a score. The score reflecting these groups and households then gets rolled into yet more algorithms and systems. The permutations are extensive, and it is not too much to state that they can be profoundly complex.

Tracking the data applied to produce or operate machine learning models requires an understanding of where and how the data has moved or processed since it was originally collected, and how it may have been used in downstream applications. This is not going to be likely something that data brokers are going to agree to engage in.

The relationship of the FCRA in the evolved scoring / machine learning context of modern data brokering

WPF's analysis is that as consumer scores proliferate, the majority of these new scores do not appear to fall under the narrow protections offered by the Fair Credit Reporting Act or the Equal Credit Opportunity Act for a variety of reasons. Scores built from factors outside a formal credit bureau file, scores designed to predict the behavior of groups of people instead of individuals, and new scores in emerging and unregulated areas may all fall outside of existing protections. For example, it is unlikely that energy consumption scores, churn scores, or identity scores would fall under the FCRA and other laws as currently written. Scores that identify the approximate credit capacity of neighborhoods instead of individuals also appear to be unregulated. As the CFPB knows, the FCRA only applies to individuals. The group / household / category workaround is an important part of the data broker ecosystem of today.

As a result consumers may have scant rights to find out what their non-FCRA consumer scores are, how the scores apply to them and with what impact, what information goes into a score, or how fair or valid or accurate the score is. Even if the input to a score is accurate, consumers do not know or have any way to know what information derived from their lifestyle, health status, and/or demographic patterns is used to infer patterns of behavior and make decisions that affect their lives.

The role of identity - particularly digital identity - in the modern data broker ecosystem

In a digitalized ecosystem, such as data broker ecosystems, digital identity is the key that unlocks just about everything, if not everything. This includes AI systems. This may surprise many, but the US does not have a formal federal digital identity ecosystem, nor federal -level regulatory governance for that system, nor regulatory leadership for that system. NIST has published its draft Identity and Access Management roadmap for digital ID in the US, but a standard alone cannot replace a formal governance structure with meaningful oversight and budgeting.[17] In today's digital world, the US actually is in an undesirable position of having to play catch-up. This has significant implications for how data brokers operate in the US.

This is particularly salient for the data broker ecosystem because identity practices in the US have been moving away from relying solely on personal contact information such as home address to link individual people to information about them. This has shifted as a result of several key factors.

First, technological capabilities have enabled the generation of new forms of data, new ways for people to interact with businesses, and new ways to make data connections. Second, regulatory restrictions on use and sharing of personally identifiable information such as names and postal addresses — along with gradual limits on the effectiveness of online cookies and other mobile identifiers — have compelled businesses to find alternative routes to establishing identity. A change that can be observed today in the data broker ecosystem is that data brokers and identity service providers are evolving to deduplicate and identify otherwise fragmented data about consumers.[18] It is notable that at least two CRAs have significant identity resolution functions.[19]

Much of this activity could be subject to regulation in other parts of the world, but it is not the case in the US. Countries in developing economies often have extremely advanced identity ecosystems, and these ecosystems are highly regulated, and come with authorities dedicated to enforcing those regulations. India, for example, has the world's most largest and most advanced identity ecosystem. It includes 1.4 billion enrollees, and it operates in near real-time to real-time.

[17] *IAM Roadmap*, NIST. https://www.nist.gov/system/files/documents/2023/05/22/NIST IAM Roadmap_FINAL_For_Publication.pdf

[18] See for example Experian's discussion regarding automotive marketing, which is not a part of its FCRA-regulated activities. *Identity resolution: link data to get a better view of your customers*, Experian (Automotive - marketing) https://www.experian.com/automotive/identity-resolution . In its discussion it discusses bringing together fragmented data.

[19] As discussed in this section, Transunion (Neustar) and Experian appear to have developed meaningful identity resolution systems. It is unclear how or if these systems are used in FCRA-regulated activities.

Biometric authentication facilitates strong authentication, and government services have been attached to the system. Each person has a unique identifying number.

Initially, the ID system, Aadhaar, introduced significant privacy problems, as researchers from WPF documented in research published in Nature - Springer, cited earlier in these comments. In 2018, the Indian Supreme Court overturned parts of India's ID law due to these problems, and required the government of India to put in place extensive technical and policy corrections to protect human autonomy and privacy. The government has done so, and the corrections are largely effective.

Now the Aadhaar identity database itself is federated, protected by a mandatory API, and enrollees can use distributed ID techniques that are built into the system to facilitate not having to share their actual ID number with businesses, however, they can still fully carry out transactions. It is an advanced digital backbone that is also privacy-preserving. A dedicated federal ministry manages the ID ecosystem, the ID system has specific federal legislation and regulations, and an ID Authority is at what would be called in the US a cabinet-level position.

This stands in contrast to the US, which has no such infrastructure in place. India's system is not perfect, but it is quite good in the post-2018 era of improvements. It is fair to say that the US has a major digital identity ecosystem problem brewing. Without leadership on how digital identity is managed and protected in the US, it will likely not be possible to solve data broker problems because of the way that data broker ecosystems are now becoming entangled with identity resolution ecosystems. The problems attached to an archaic and comparably unregulated digital ID system could become problematic fairly quickly. These same issues could also be critical in thinking about how to ensure that digital wallets do not become a playground for mischief by players that are not part of the financial services ecosystem or are unregulated.

The limits of privacy in the US ID ecosystem of today and how it relates to data brokering

Consider for example, companies operating in the identity ecosystem that have installed what they consider to be safeguards protecting user data privacy, such as obscuring email addresses and phone numbers through hashing or encryption techniques before the data are shared, [20] or conducting data sharing in so-called "clean room" environments.[21] This sounds good on first blush. However, in some cases, including cases involving regulated Credit Reporting Agencies, hashed email addresses can be used as an identity artifact. This means that an email that has been hashed can become just as good as a name, with work. To quote the literature, a hashed email address can be an "Authenticated starting point for cross-device identity resolution" that "can function like a digital passport that traces every behavior and action a customer takes when logged into an account that is authenticated with an email, making hashed emails a

[20] *Hashing Identifiers,* Liveramp. https://docs.liveramp.com/connect/en/hashing-identifiers.html.

[21] See for example LiveRamp's mention of clean rooms. *LiveRamp enables identity and advanced activation in Snowflake*, LiveRamp. 27 February 2023. https://investors.liveramp.com/news-and-events/press-release-details/2023/LiveRamp-Enables-Identity-and-Advanced-Activation-in-Snowflake/default.aspx .

goldmine for customer data." [22]

Identity service providers are reliant on certain match partners to provide consumers with the ability to opt out from the use of their personal information,[23] but as discussed in these comments, opting out is not a serious option in data broker systems using AI, scores, and other machine learning techniques. Industry distinctions between "personal data" and unique or "pseudonymous" identifiers are blurry. And the increasingly multi-layered and interlinked design of the identity ecosystem (digital wallets - credit and debit cards - CRAs that have potential capacity to cross-walk data) could render such opt-out practices ineffectual as meaningful privacy protections.
ODNI

It is also worth reiterating that techniques employed in an attempt to de-identify or anonymize data are not always reliable. As noted above, even a National Intelligence Senior Advisory Group report on commercial available data use by national intelligence agencies states that commercially-available data "can also be combined, or used with other non-CAI data, to reverse engineer identities or de-anonymize various forms of information."[24]

III. Conclusion

Looking at the past, WPF sees missed opportunities. Looking at the present, we see an extraordinary task before all of us if we want to solve problems for consumers regarding data brokers. Data brokering is built deeply into modern business processes today. The US government is using commercially available data from data brokers. The US lacks appropriate governance for its digital identity ecosystem, which is just now emerging. Of meaningful concern is the interactions between digital identity resolution, the data broker space, and the line between regulated and unregulated data.

WPF does see solutions.

- A key solution is to ensure that additional, modern forms of eligibility are added to the FCRA's roster of what qualifies as eligibility.

- Also key is to ensure that the emerging "household" loophole is closed. If a score, like an aggregate credit score that is unregulated because it does not use regulated data elements,

[22] *Uncovering hashed email: you may be sitting on a goldmine of customer data and don't even know it*, Experian. 25 August 2021. https://www.experian.com/blogs/marketing-forward/uncovering-hashed-email/ .

[23] Privacy Policy, TransUnion.com / Neustar, note of "Match Partners" in categories of sources. https://www.transunion.com/privacy/neustar .

[24] *Report from the Office of Director of National Intelligence Senior Advisory Group Panel on Commercially Available Data*, approved for release 5 June 2023. https://www.odni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf . See pp. 1 and 5.

but it nevertheless acts as a form of a credit score, then these kinds of scores need to be brought under the FCRA.

- Modernized de-identification standards would help, as would rules that do prohibit the use of deidentified data for classifying consumers into certain types of groups which have eligibility or eligibility-adjacent implications. (Such as acceptance into an educational institution, such as a college.)

- A regulated digital ID ecosystem will be necessary, sooner rather than later.

- Also, public sector guardrails for the federal government would be welcome. There is no reason why rules for the public sector would not also apply to government agencies. WPF recognizes that National Security interests would likely need slightly different guidelines, but guidelines will still be necessary.

The World Privacy Forum urges CFPB to act on these issues; the World Privacy Forum appreciates the opportunity to respond to the RFI, and we look forward to offering assistance and working with you to make progress.

Respectfully submitted,

Pam Dixon, Executive Director, World Privacy Forum

Kate Kaye, Deputy Director, World Privacy Forum

Appendix

WPF developed a taxonomy in 2014 to understand how data brokers were using consumer scores. These scores are not regulated under the FCRA.

Score Taxonomy

In minds of consumers, there is just one score, the credit score. But the credit score is just one final outcropping of a layered and complex taxonomy of scoring. This taxonomy can assist consumers in seeing the full range and depth of scoring activities that exist, and may impact them.

I. Predictive Statistical Models

II. Formal Scoring Models

III. Consumer Scoring Models

IV. Consumer Scoring Model Type (application, behavioral, or combined)

V. Consumer Scoring Function: the broad function of the score card, as follows:

***Propensity* score** cards: will the consumer, for example, default, what is the propensity of a certain result. Credit scoring is a propensity scoring function. Health Scoring is a propensity function if it falls under the full taxonomy preceding this point.

***Response* score** cards: will the consumer respond to a direct marketing offer

***Usage* score** cards: will the consumer use the credit (or other) product if given the product

***Attrition* score** cards: will the consumer continue with the lender, especially if there is some special offer available for an introductory period only.
Customer profit scoring score cards: estimates the total profitability of the customer to the lender

Product profit score cards: seeks to estimate the profit the lender makes on this product from the customer

VI. Source of the Score Model and score (Generic, custom, or vendor supplied score) VII. The Specific Type of Score (fraud, credit, etc.) Here, the term credit refers to the broad type of score.

VIII. Application of Score (what purpose is the score used for)
Consumer-related: test: does the score impact a decision about an individual consumer or a group of consumers?
Research-related: (esp. Health research) test: is the score used to primarily to understand or explain a process or a disease and never used to make a decision about an individual consumer beyond a clinical medical decision? (If a financial or risk decision is taken, then the score becomes a consumer score, not just a clinical score.)

IX. Actual Scores (This includes all specific scores resulting from the taxonomy, Z score, Falcon score, FICO score, etc.) Note: this report is focused on Consumer- related scores, or scores that are used for consumer purposes. If at any point a pure research-related score is used in a consumer score model as a predictive factor and the resulting final score is used for consumer purposes, the final score would be considered a blended consumer score and would be included in the consumer category. See Taxonomy step VII.

zoominfo [redacted]

[redacted]
zoominfo.com

June 25, 2024

California Privacy Protection Agency Board
2101 Arena Blvd.
Sacramento, CA 95834

RE: Preliminary Comment DROP 06-24

Dear CPPA Board:

We appreciate the opportunity to offer comments on the emerging rulemaking to develop and deploy an Accessible Deletion Mechanism (ADM). ZoomInfo has long been a privacy-forward company, and we fully support the Agency's efforts to enhance privacy protections for California consumers.

ZoomInfo is a business-to-business (B2B) platform that collects, curates and makes available information about companies and the professionals within them. Our customers are companies that sell to other companies. As a company focused on B2B data, our comments aim to illuminate the considerations that affect B2B data brokers and the specific professional information we handle.

Personal vs. professional personas

Many individuals maintain distinct personal and professional personas. The data connected to an individual's personal persona poses a different level of sensitivity and risk than information related to their professional persona. The former can be used to track movement, access private accounts, or assume identities. This type of information can include data such as precise geolocation, health information, financial information, and account numbers and passwords, and it is widely regarded as highly sensitive.

However, professional information—similar to what people typically put on a business card or resume—is not sensitive nor is it intended to be private. Business information is inherently low-risk and broadly accepted as information that is intended to be shared among professionals, for professional purposes. Tens of millions of professionals readily share work-related information every day by distributing it to colleagues, posting it on company websites, or publishing it on professional networking sites.

It is no surprise, then, that the intent of SB 362 (Delete Act) is focused on information relating to an individual's personal persona. In April 2023, the bill's sponsor Senator Josh Becker invited several advocates to a Judiciary hearing to speak alongside him in support of the legislation. The example use cases that were shared in that hearing made evident that the intention of SB 362 was to protect against use cases that could put an individual at risk. These examples included law enforcement purchasing geolocation instead of getting a warrant, and instances of data brokers selling prayer or political information as well as personal information that could be used for stalking.

The distinction between personal and professional contexts has been recognized in Vermont - the first state to operationalize a Data Broker registry - making clear that the intention was to safeguard information related to a consumer's *personal* persona and not their professional persona:

> *(B)"Brokered personal information" does not include publicly available information to the extent that it is related to a consumer's business or profession. For example, a doctor's office address or phone number is not BPI, but a doctor's home phone number (assuming it is not used for business) is BPI. The idea behind this exemption is that while people have a privacy interest in their personal information, they generally do not want to keep their business contact information private. The purpose of this exemption was to exclude entities that publish business directories, professional websites, politician contact lists, and other such collections of information that do not raise privacy concerns.*[1]

Notice & choice; fully informed deletion requests

In light of the stark differences in sensitivity, risk, and use of personal and professional information, it is imperative that consumers be explicitly informed about the impact of their ADM requests. In offering consumers a welcome "one stop shopping" experience for deleting their information from California data broker systems, consumers should not be faced with an "all or nothing" choice that enables deletion of information about their personal persona, at the cost of reducing their professional visibility.

Many reasonable consumers want data brokers to delete whatever personal information data brokers may have surreptitiously gathered about them online or through other means. However, it does not naturally follow that those individuals also want information about their business and their professional role to be removed from a professional directory. By removing their business information, a person may miss recruitment opportunities for themselves, or for employees they need, or miss buyer opportunities because they and/or their business can no longer be found in a professional database.

We suggest that consumers be provided information and a mechanism to choose whether their request should affect information related to their professional persona, in addition to information about their personal persona. Providing this information and optionality will guard against inadvertent impacts to Californians' professional lives, where individuals may seek only to safeguard sensitive data relating to their personal personas.

[1] *Guidance on Vermont's Act 171 of 2018 Data Broker Regulation*, Vermont Office of the Attorney General, page 5 (December 11, 2018), *available at* https://ago.vermont.gov/sites/ago/files/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf. *See also* 9 V.S.A. § 2430(4)(B).

Verification; clear parameters for business-to-business data brokers

Successful deployment of the ADM must ensure that data brokers can sufficiently meet the requirements of the Delete Act. It is important to recognize that B2B data brokers like ZoomInfo process and identify individuals using different data points from other data brokers, and that this distinction may pose challenges in our ability to fulfill some requests.

B2B data brokers process information related to individuals' professional personas, such as their job titles, employers, business email addresses and business phone numbers. In order for a company like ZoomInfo to successfully fulfill a data subject's verified request, the request must include information that matches these types of professional data points. Without a business-related data point, data brokers that process information related to business personas may not be able to accurately identify the data subject and fulfill the request. For example, a request that includes only a common name and a personal email address would not permit ZoomInfo to process a deletion request.

As discussed above, we recommend consumers be given an informed opportunity to exclude professional information from the ambit of their deletion requests. To the extent that individuals choose to delete their professional data, we recommend that the ADM requires them to input business-related contact information, such as their business email address, so that companies processing B2B data can fulfill their requests.

We also encourage the agency to state explicitly in its rulemaking that companies are not obligated to fulfill requests where the information provided about a consumer is not sufficient to identify them—for example, where a request received by a B2B broker includes only a personal email address instead of business email.

Very truly yours,

Kristin M. Malone
Deputy General Counsel
ZoomInfo Technologies

ZoomInfo (NASDAQ:ZI) is a Go-To-Market Intelligence Solution for more than 35,000 companies worldwide. The ZoomInfo platform empowers business-to-business sales, marketing, and recruiting professionals to hit their number by pairing best-in-class technology with unrivaled data coverage, accuracy, and depth of company and contact information. With integrations embedded into workflows and technology stacks, including the leading CRM, Sales Engagement, Marketing Automation, and

Talent Management applications, ZoomInfo drives more predictable, accelerated, and sustainable growth for its customers. ZoomInfo emphasizes GDPR and CCPA compliance. In addition to creating the industry's first proactive notice program, the company is a registered data broker with the states of California and Vermont. Read about ZoomInfo's commitment to compliance, privacy, and security. For more information about our leading Go-To-Market Intelligence Solution, and how it helps sales, marketing, and recruiting professionals, please visit www.zoominfo.com.