CCPA: The Right of “Deletion”

Webinar No. 5 of IAB’s Privacy Law Webinar Series

June 11, 2020
Today’s Speakers

Alex Cone
Senior Director, Product Management
IAB Tech Lab

Andrea Giannangelo
CEO, Founder, and Head of Product
Iubenda

Michael Hahn
SVP & General Counsel
IAB & IAB Tech Lab

Stephanie Hanson
Offering Manager
OneTrust

Jessica Lee
Co-Chair Privacy, Security, and Data Innovations
Loeb & Loeb LLP
Right to Disclosure
Right to Deletion
Right to Opt-Out (Do Not Sell)
Right to Nondiscrimination
Data Deletion Request Handling

Summary

This specification defines the Data Deletion Request (DDR), which is the mechanism by which the IAB CCPA Compliance Framework complies with Section 1798.105(c) of the California Consumer Protection Act (CCPA) which states “a business that receives a verifiable consumer request from a consumer to delete the consumer’s personal information shall ... direct any service providers to delete the consumer’s personal information from their records.” The DDR is a technical contract between a Publisher and Vendors in order to enable a consumer on a Publisher’s digital property to direct Vendors to delete the consumer’s personal information from their records. As stated, the DDR exists primarily to comply with CCPA but may be used for deletion requests outside the domain of CCPA governance.

The technical solution detailed in this specification provides the means to signal consumer requests for data deletion. Companies supporting the US Privacy Framework (i.e., service providers) will respond to the signals by deleting the consumer’s relevant personal data to the extent required by CCPA. The process for deletion depends on the company’s technology and operational practices in place. How a Vendor deletes a consumer’s personal data is out of scope for this specification.

Relevant Documents

Limited Service Provider Agreement (12-2-19 version)
OneTrust CMP Integration for Data Deletion Requests

Reach out to us at shanson@onetrust.com
I. Right to Deletion Summary

“Request to delete” means a consumer request that a business delete personal information about the consumer that the business has collected.

- Collected from the consumer versus in a sale

Business Obligations

- Upon a “verifiable consumer request,” businesses must (i) delete any personal information about that consumer from its records and (ii) direct any service providers to delete that consumer’s personal information from their records.
- Request must be fulfilled within 45 (calendar) days from the day the request is received (extension allowed for an additional 45 days when reasonably necessary, must give notice of delay and accompanying reasons to consumer within initial 45 days).
- The regulations require businesses to confirm request receipt within 10 business days and provide information about how the business will process the request.
- If the business cannot verify the consumer within the 45-day time period, the business may deny the request.
I. Right to Deletion Summary

Service Provider Obligations
• Service providers must delete a consumer’s personal information as directed by the business.
• No express timeframe given for deletion but presumably within same 45-day period.

Exceptions
• Businesses and service providers need not comply with a request to delete personal information if retention is necessary for:

(1) completing a transaction, (2) detecting security incidents/protecting against illegal activity, (3) debugging to identify and repair errors, (4) exercising of free speech, (5) complying with the California ECPA, (6) research (if consumer has provided informed consent), (7) “solely internal uses” reasonably aligned with consumer expectations, (8) legal compliance, and (9) internal use compatible with the context in which the consumer provided the information.
II. Submitting Deletion Requests

A business shall:

• Disclose the right of deletion within its privacy policy
• Provide at least two methods for submitting a request, as described in privacy policy
  • business **may** use a two-step process for online requests to delete where the consumer must first, submit the request to delete and then second, separately confirm that they want their personal information deleted.
• When providing these methods, take into account the means by which the business primarily interacts with customer
• Not require the creation of an account for submitting a request
III. What is a “Verifiable Consumer Request”?

• A “verifiable consumer request” is a request that a business can reasonably verify is made by:
  (i) a consumer,
  (ii) a consumer on behalf of the consumer’s minor child, or
  (iii) by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf.
III. What is a “Verifiable Consumer Request”?

According to the regulations:

• The business shall establish and document a reasonable method for verifying a consumer request.

• **Taking into account the sensitivity of the personal information and risk of harm to consumer posed by unauthorized deletion**, the business shall verify a consumer’s identity to either (i) a “reasonable” degree or (ii) a “reasonably high” degree of certainty.
  
  o **A “reasonable” degree of certainty**: May include cross-referencing at least two pieces of personal information provided by consumer with personal information held by business.
  
  o **A “reasonably high” degree of certainty**: May include cross-referencing at least three pieces of personal information provided by consumer with personal information held by business.

• Businesses can require *existing* accountholders to submit requests through such accounts.
IV. Denying a Request

• The business shall inform the consumer of any rejection, including the reasons for such rejection and any rights the consumer may have to appeal the decision.

• Where relying on a deletion exemption as the basis for denial, the business must:
  o Inform the consumer that it will not comply with the consumer’s request and describe the basis for the denial
  o Delete the consumer’s personal information that is not subject to the exception
  o Only use the retained information for purposes of the exception.

• Where the business denies a request, and the business sells that consumer’s personal information, the business “shall ask [in such notification of denial] the consumer if they would like to opt out of the sale of their personal information and include either the contents of, or link to, the notice of right to opt-out…”

• In either case of granting or rejecting a request, the business must maintain records of consumer requests for 24 months and notify the consumer that such record will be maintained.
V. Fulfilling A Request

What exactly is “deletion”?  
• According to the draft regulations, a business can comply with deletion requests by:
  
  o Permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems;
  
  o De-identifying the personal information; or
  
  o Aggregating the personal information.
V. Fulfilling A Request

• If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer’s request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose.

• If the business complies with the consumer’s request, the business shall inform the consumer that it will maintain a record of the request.

• A business may retain a record of the request for the purpose of ensuring that the consumer’s personal information remains deleted from the business’s records.

• In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered and more prominently presented than the other choices.
VI. Service Provider Deletion

• If a service provider receives a request to know or a request to delete from a consumer, the service provider shall either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.
  • **There is no affirmative obligation for businesses to confirm deletion**
• Limitations of liability
  o Businesses do not have liability for their service providers’ use of personal information in violation of its contractual restrictions
  o A businesses must not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation.
  o The same is likewise true for service providers in relation to businesses.
VII. The IAB LSPA and Deletion Right

• The role of service providers under the IAB Limited Service Provider Agreement (LSPA) upon consumer opting out via the “Do Not Sell” link on a business’s site (e.g., publisher digital property).

• Scope of obligation and practical challenges
  o LSPA rep and warranty around deletion
  o Challenges in businesses passing the deletion request to service providers
  o The Tech Lab’s specification addresses practical challenges
First, a little about Tech Lab...
Engage a member community globally to develop foundational technology and standards that enable growth and trust in the digital media ecosystem.
Engage a member community globally to develop foundational technology and standards that enable growth and trust in the digital media ecosystem.

Member-driven, member-developed:
- 750+ companies
- 20+ working groups
- 2500+ participants
- 40+ countries

Sharing the cost, sharing the benefits

Broad availability & utility, by design

We live this – as a neutral, transparent, open-source, non-profit org
What Are Technical Standards? We All Rely on Them...

Tech Lab standards are similar...but for digital media.

Standards & compliance help our industry improve interoperability, which:

- Increases product development **efficiency & quality**
- Enables rapid **scale**
- Frees resources for **innovation**
- Helps **mitigate risks**
- ...and fuels **growth**
Now, what about delete requests...
One-off delete protocols are **expensive**
One-off delete protocols are error-prone.
Problem

One-off delete protocols **do not scale**

× 5, 10, 50...
Problem

One-off delete protocols **do not scale**

× 50, 500, 5000...
CCPA/US Privacy Technical Working group

- 182 member participants
- Technologists + policy/legal
Delete Request Handling Specification
Over 60,000 clients in 100+ countries

- **Self-updating** Privacy Policy and Terms and Conditions
- Cookie Consent Management
- Proof of Consent API
- GDPR & CCPA

For CCPA: [www.iubenda.com/ccpa](http://www.iubenda.com/ccpa)
Data Deletion Request Handling
WHAT YOU NEED TO KNOW

• It’s part of the US Privacy API
• It’s a web specification, but it also supports non-web
• It provides the tools to scope deletion requests down to the single publisher and to the single user
HOW DOES IT WORK

- The **vendor** creates a js script that, when executed, performs the data deletion.
- The **publisher** hosts all of its vendors’ scripts on a page where the user will initiate the data deletion request.
HOW DOES IT WORK

• When the user hits the “Data Deletion” button, the US Privacy API is called and all vendors’ scripts are notified
• For non-web, identifiers of the app and of the user are sent with the request
• Each vendor has access to both the user and the publisher and can narrow down the data deletion scope to the minimum
Andrea Giannangelo
Head of Product at iubenda
IAB Tech Lab contributor
andrea@iubenda.com