
LifeCorp Office of Public Policy

Consumer Attention Protection Framework: CAPA Discussion Draft

VEIL-P-26 · Proposed Consumer Attention Protection and Advertising Interoperability Act.

Policy purpose and consultation status

Protection that depends on individual configuration is protection for the few. VEIL makes protection a property of the platform.

The Consumer Attention Protection and Advertising Interoperability Act is a proposed legislative framework offered for consultation. LifeCorp seeks a common interface that reduces tracking exposure, limits execution costs and supplies an accountable institutional basis for browser-mediated advertising. CAPA remains a discussion draft; enactment and enforcement would require the competent public authorities' separate processes.

1 — Standardized advertising interfaces

Participating publishers would request advertising through an interoperable browser interface using defined placement fields and resource envelopes. The standard-setting process should publish implementation requirements, version changes and access conditions. Equivalent conforming implementations should be able to exchange supported requests.

The interface should reduce duplicated delivery infrastructure while preserving a practical migration route for publishers. Transition assessment should include smaller sites whose operational capacity differs from that of major advertising intermediaries.

2 — Browser mediation and execution limits

Certified browsers would mediate retrieval, rendering and suppression within isolated execution environments. Mandatory resource ceilings would address computation, memory, network use and disruptive presentation. Implementations should expose testable failure behavior when a request exceeds those limits.

Evaluation should cover ordinary device constraints as well as high-capacity environments. Certification requirements would identify the enforcement properties actually tested and the residual risks retained by a specific implementation.

3 — Publisher privacy and individual-state confidentiality

Publisher-facing identifiers would be opaque and scoped to the relevant placement context. Individual advertising preferences and suppression state would remain under mediator administration rather than routine publisher inspection. Access to measurement information would follow an explicit purpose and retention boundary.

Threat-model publications should address repeated observations, collusion and device-dependent side channels. The framework seeks measurable confidentiality properties with disclosed limitations, including the inferences still possible from an otherwise standardized request.

4 — Certification and independent assurance

An open certification profile would define implementation tests, reporting requirements and renewal conditions. Independent assurance should examine resource limits, state confidentiality, settlement integrity and the operation of policy controls. Funding relationships and unresolved findings should accompany the certification record.

Consultation should determine affordable access for small implementations, recognition of equivalent testing and safeguards against concentrated control of the certification process. Common standards require a credible route for new entrants to demonstrate conformity.

5 — User and enterprise policy authority

Individuals would select an advertising preference from the service levels available within their governing environment. In a managed enterprise environment, an authorized sponsoring organization could define the permitted policy set, its review period and the responsible administrative contact. The browser would enforce the valid selection within that set.

Policy records should identify the institution assigning the available levels and provide a usable appeal route. Consultation remains open on the circumstances in which an employer or service administrator may constrain individual suppression choices and the protections required for affected users.

6 — Mediation integrity and anti-circumvention

The draft would prohibit mediation bypass: modification of a certified client that changes delivery or suppression decisions outside the approved policy interface. Integrity enforcement would apply to the certified mediation boundary and its defined reporting behavior. Exceptions, remedies and proportionate enforcement would be specified through the implementing process.

The scope of the provision requires public review, including its application to independent extensions and user-installed filters. The framework should identify how legitimate testing, accessibility tools and appeals can proceed within a consistent assurance model.

7 — Privacy-preserving measurement and settlement

Reporting would distinguish requested placements, attempted delivery, rendered advertisements and verified views. Suppressed delivery would remain outside verified-view billing. A settlement profile should define the evidence available to publishers, delivery services and independent auditors without exposing an individual's cross-site history.

Fraud prevention and billing integrity require further technical work. The programme should publish disputed measurement cases and the procedure for resolving them. Certification would attach to a defined reporting profile rather than an undifferentiated claim of accurate measurement.

8 — Interoperability, enforcement, appeals and transition

Implementation should proceed through published interoperability tests and realistic migration periods. Users, publishers and browser vendors should have routes to challenge an authority assignment, a conformity finding or an enforcement decision. Regulatory powers would remain with the institutions established by any future law.

LifeCorp invites responses on user control, implementation diversity, certification costs and the draft's allocation of policy authority. The technical case for browser mediation and the institutional case for a restriction on bypass require separate evidence and deliberation.

Supporting publications

<https://lifecorp.org/archive/veil-fragmented-attention>

<https://lifecorp.org/archive/veil-protocol>

<https://lifecorp.org/archive/veil-assurance>