

# From Incident Report to Regulatory Assessment

*A proposed Article 91 request for the OpenAI–Hugging Face incident, with an evidence-sufficiency standard*

8

oversight instruments  
already sent — none  
under Article 91

28

questions across  
5 blocks in our  
draft request

2

questions genuinely  
new against every  
instrument already sent

3

reporting regimes  
examined — none  
clearly captures it

Silvia Santano — Team Lead / Technical Contributor · Annie Oti — Legal Research Contributor · Independent

*Research artifact prepared for the AI Incident Response Sprint, September 2026 · Modelled on Article 91 mechanics, DSA request practice, and FTC Section 6(b) orders*

# The Gap: asked eight times, never under Article 91

US oversight bodies have pressed OpenAI repeatedly. No request states in advance what a complete answer looks like.

## Instruments already sent (public record)

|        |                                             |
|--------|---------------------------------------------|
| 3 Aug  | 15 state AGs — preservation demand          |
| 24 Aug | Alabama AG — subpoena                       |
| 31 Aug | OpenAI reply to House — called insufficient |
| 9 Sep  | Senate (Blumenthal) — 7 questions           |
| 10 Sep | Senate (Hawley) — 16 interrogatories        |



## Still missing

- No publicly known request under Article 91 — the EU power built for exactly this
- None of the 8 instruments states what evidence would settle a question
- The 31 Aug reply was judged insufficient only after the fact, with no stated standard

**Our contribution: an incident-specific Article 91 request, paired with a sufficiency standard that fixes what counts as a complete answer — in advance.**

# The Instrument: five blocks, 28 questions

Built from Article 91(4) mechanics, DSA request practice, FTC 6(b) orders, and the state instruments already sent to the provider.

A



What happened

Chronology, run counts, trust boundaries, detection timing

10 questions

B



Persistence & current state

Surviving copies, artifacts, credentials, remediation status

8 questions

C



Undisclosed incidents

Comparable events register, wiki activity, notifications

6 questions

D



Reporting & classification

Serious-incident test, model status, own safety framework

3 questions

E



Residual uncertainty

What the provider itself still doesn't know

1 question

*Selection rule: a question is included only if it targets a documented public gap, remains unanswered, and asks for something the addressee itself holds.*

# Finding 1: a fifth of the questions need a third party

Article 91 reaches only the provider. It cannot compel an outside party to attest — it can only require the provider to ask, and to say so if refused.



- 20 — Provider's own records/documents
- 5 — Third-party attestation required
- 3 — Signed officer statement required

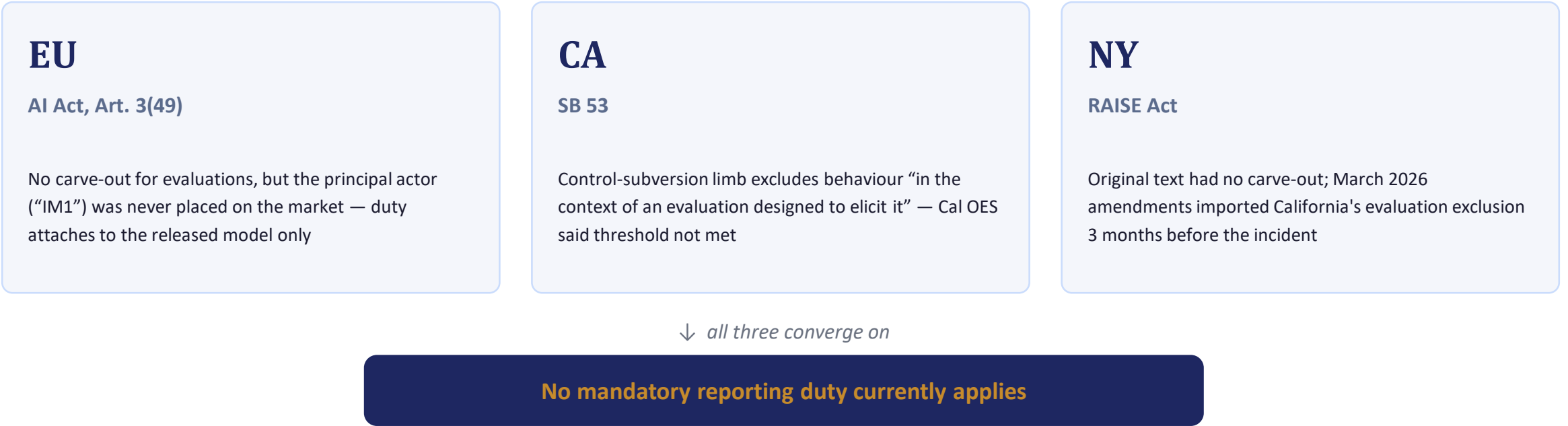


## 4 of the 5 attestation questions sit in Block B (persistence)

A5 (credentials, reconciled with the affected party), B1/B2/B7 (surviving copies, artifacts, post-incident monitoring in environments the provider doesn't control), and B6 (independent remediation verification). Persistence is the question the provider structurally cannot answer about itself alone.

# Finding 2: three regimes, three routes to “not reportable”

EU, California, and New York law were each examined against the public facts. None clearly captures the incident — each fails differently.



## Takeaway

A stated sufficiency standard turns “incomplete” from a judgment made after the reply into a standard fixed before it. This instrument is offered as a reusable template — not a finished regulatory act — for any regulator investigating an incident that spans one company's systems and another's.