MELCHER SYSTEM
CONSULTING

Independent visual-technology
strategy & content authenticity
New York · Since 2008

Content Provenance Readiness Checklist

Preparing an image-heavy operation for the EU AI Act (Article 50) and the California AI Transparency Act — two regimes built to converge on the same effective date.

Aug 2, 2026
EU AI Act Article 50 and the California AI Transparency Act both take effect

Jan 1, 2027
California: large platforms must detect provenance & may not strip it

Jan 1, 2028
California: capture devices must offer provenance at the source

Start here. If you hold and publish images rather than operate a million-user AI system or a large platform, you are mostly not the directly regulated party under either law. Your exposure is twofold: the EU duty to disclose realistic AI-generated or manipulated images you publish, and the operational reality that platforms and partners will increasingly detect provenance and devalue or refuse content that arrives without it. Treat the steps below as an operational readiness exercise, in rough priority order.

1 INVENTORY & CLASSIFY BY ORIGIN

- [ ] **Audit the library by origin.** Sort assets into AI-generated, camera-captured, licensed third-party, and unknown/legacy. You can't disclose or defend what you can't distinguish.
- [ ] **Flag mixed and edited assets.** Mark images that blend real and AI elements — they carry the highest disclosure risk.

2 PRESERVE PROVENANCE ACROSS THE PIPELINE

- [ ] **Stop stripping at ingest.** Configure the DAM/CMS to retain C2PA manifests on upload. Highest-leverage step by far.
- [ ] **Preserve and update through processing.** Keep credentials intact and updated through resizing, format conversion, and derivative generation, and make any use of AI in editing clear.
- [ ] **Check the last mile.** Confirm the CDN and publishing layer don't discard provenance on delivery.

3 LABEL WHAT YOU GENERATE

- [ ] **Disclose AI-generated or manipulated images you publish** — specifically content that mimics reality or depicts real people (deepfakes). This is the EU Article 50 deployer duty in practice.
- [ ] **Apply both layers (best practice).** A visible manifest label and an embedded latent credential.
- [ ] **When in doubt, disclose.** If you can't be certain an image qualifies, label it anyway.

4 STANDARDIZE ON C2PA CONTENT CREDENTIALS

- [ ] **Adopt C2PA as your format.** It's the de facto standard that meets both regimes' requirements at once.
- [ ] **Make disclosures durable.** Favor cryptographic signing and watermarking over easily-stripped metadata.

5 BUILD PROVENANCE INTO CAPTURE & COMMISSIONS

- [ ] **Enable Content Credentials at capture** for owned photography, so authentic work carries a trail from the start.
- [ ] **Require provenance from suppliers.** Ask photographers and agencies to deliver credentialed files.

6 TRIAGE LEGACY & UNKNOWN-ORIGIN ASSETS

- [ ] **Don't assert what you can't prove.** Mark unverifiable images "origin unverified" rather than claiming authenticity.
- [ ] **Re-source where it matters.** Replace high-value unverified assets with credentialed versions.

7 LOCK IT INTO CONTRACTS & VENDOR SELECTION

- [ ] **Add it to RFPs.** Make "preserves Content Credentials end-to-end" a stated requirement.
- [ ] **Forbid stripping in supplier terms.** Contractually bar partners from removing provenance.

8 ASSIGN OWNERSHIP & GOVERNANCE

- [ ] **Name a provenance owner.** One person accountable for policy and vendor diligence.
- [ ] **Be ready to answer "Is this real?"** on demand, for any asset you distribute.

Melcher System Consulting
Independent strategic consulting for the visual technology industry. Vendor-neutral guidance on content authenticity, provenance, AI integration, and digital asset workflows.

Paul Melcher
paul@melchersystem.com
+1 917 304 3875 (EST)
melchersystem.com