



A nutrition label for all the content you've ever made

How C2PA, content provenance, and the
AI-powered supply chain are rewriting the rules
of modern marketing



The age of the fake

In the spring of 2024 a photograph appeared on the homepage of a Fortune 100 consumer goods company. It showed a woman laughing in a sun-drenched kitchen as she poured olive oil over a salad so vibrant it practically hummed with Mediterranean warmth. **The image was beautiful. It was also, in every meaningful sense of the word, a lie.**

Nobody had stood in that kitchen. Nobody had poured that oil. No photographer had adjusted the light, no food stylist had arranged the basil leaves just so. The entire scene—woman, kitchen, oil, salad, sunlight—had been generated in **eleven seconds by a text-to-image model**. It had been **approved** by a junior brand manager, **uploaded** to a Digital Asset Management (DAM) system, and **pushed live to forty-seven markets in nineteen languages**. Within a week, it had been seen by an estimated fourteen million people. None of them knew that the image had been artificially generated, and no one had any way to check.

Enterprise brands now produce content at a scale that would have been unthinkable a decade ago. Companies operating at the frontier—the Nestlés, the Unilevers, the Procter & Gambles—generate more than a million digital assets a year, in dozens of languages, for hundreds of channels, across thousands of product lines, at a pace that has turned their marketing operations into something closer to industrial manufacturing than the creative craft it once was.

And now generative AI has entered the arena.



Leading CPG companies generate more than a million of assets per year

C2PA: an anti-fake coalition

An emerging technical standard is addressing this new reality yet there is so far little awareness of it in marketing. It's the Coalition for Content Provenance and Authenticity (C2PA) and it may turn out to be the most consequential infrastructure move made in marketing this decade.

C2PA might be seen as a nutrition label for digital content. In the same way as a cereal box tells you exactly what's inside – the sugar, the fibre, the sodium – **C2PA attaches a tamper-evident manifest to every piece of media**. It records who created the content, what tools were used, whether AI was involved, and what edits were made, and by whom. This information is **cryptographically sealed into the file itself. It travels with the asset wherever it goes**—from a photographer's camera to a Digital Asset Manager (DAM), content management system (CMS), social platform and, finally, a consumer's screen.

The coalition behind it reads like a who's who of the digital supply chain: **Adobe, Microsoft, Google, Amazon, Meta, OpenAI, Intel, the BBC, Sony, Nikon, Leica. Publicis Groupe** has joined as the first advertising holding company on the steering committee. The community now exceeds **6,000 members**. Hardware manufacturers are embedding provenance at the point of capture. **Google's Pixel 10** recently achieved the highest tier of C2PA security compliance. And in late 2025 the official Content Credentials icon, a minimalist "CR" pin, was introduced with the ambition of becoming as universally recognised as the copyright symbol.

Deloitte, too, is a member of the coalition, because this is a **business transformation conversation, not just a technical one**. Content advisors (whether technical, operational or strategic) are now accountable for making supply chains provenance ready. This has become a core responsibility.

Provenance regulation is reshaping Content Supply Chains and ways of working. Early adopters will turn this into competitive advantage; others will treat it as a cost of doing business.



Three forces behind a content tipping point

“The tipping point is that magic moment when an idea, trend, or social behaviour crosses a threshold, tips, and spreads like wildfire,” writes Malcolm Gladwell in his book, *Tipping point*, published in 2000. C2PA is at exactly that point. Three forces are pushing it from nice to have to non-negotiable.

Force One: *The Regulatory Wave.*

The EU AI Act's Article 50 will require providers of generative AI systems to label all AI-generated content in a machine-readable format by August 2026. The European Commission has published a first draft of the Code of Practice on Transparency, which explicitly calls for a multilayered approach—metadata embedding, watermarking, content credentials. The draft proposes a standardised “AI” icon that must be visible at first exposure for deepfakes, synthetic video, and AI-generated text on matters of public interest. This is a legal requirement, not an optional guideline.



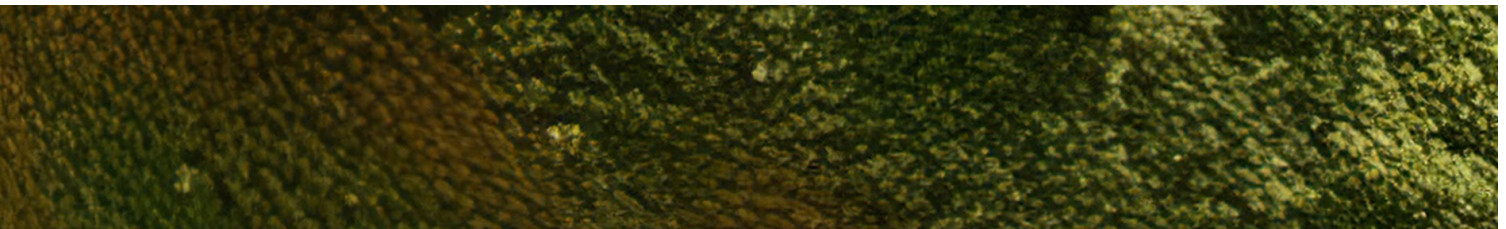
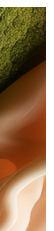
Force Two: *The Trust Deficit.*

Consumer trust in digital content has collapsed. In an environment where an image of a papal fashion moment can go viral before anyone confirms it's AI-generated, scepticism has become standard. This represents an existential threat to brands. Advertising has always been a trust transaction: I show you something, you believe it enough to act. When the medium itself is suspect, every brand message suffers. In a world of synthetic everything, even the most authentic content feels manufactured.



Force Three: *The Scale Problem.*

When you produce a million assets a year, you lose the luxury of knowing where they came from. Your DAM holds stock from fourteen agencies, AI variants from three models, licensed user content, and heritage assets stripped from metadata. Identifying the source of content is a supply chain problem that demands supply chain solutions.





AI to free the creative mind, not threaten it

Embedding content credentials into every asset changes the game. Suddenly, your DAM doesn't just store files—it stores **verifiable chain-of-custody**. You can audit every image in every market to determine which are human-created, AI-generated, or hybrid. You can trace a rogue asset back to the exact moment it was modified and identify the tool that was used. **Your compliance team automates EU AI Act labelling at publication.** Your brand safety team verifies **that influencer content actually came from whoever claims to have made it.** You can then manage your customers' trust.

Agentic AI can supercharge this process, not just by following instructions, but by running the show. An AI agent takes a brief and handles the rest: forty-seven localised variants, brand compliance

checks, approval routing, scheduling, performance tracking. Minimal (but key) human intervention. Maximum output. Organisations piloting this approach are achieving 70% faster time to market. What before took six months can now be done in less than eight weeks.

C2PA can become your operating system of trust. Every AI move is logged, every tweak signed, every hand-off documented. The whole chain becomes transparent and tamper-proof.

In Deloitte's view, transparency and speed are not trade-offs, but partners. The AI operational machinery frees the human creative mind to do what it does best—make work that influences people. The technology doesn't replace the craft; it protects it.

C2PA is also a cybersecurity defence

There are risks around content of which most marketing leaders are, as yet, unaware. Yet the numbers are stark. In 2025, AI powered deepfakes featured in more than thirty percent of high-impact corporate impersonation attacks. Deep-fake and executive impersonation scams provoked in excess of 200 million dollars in losses globally in Q1 alone. Gartner found **43 percent of cybersecurity leaders had experienced a deepfake audio incident**; Deloitte projects 40 billion dollars in AI-enabled fraud globally by 2027 in US banking alone.

A brand might produce a million assets a year, and **every image, video, and audio clip is raw material for an attacker.** Your CEO's keynote can be cloned into a fraudulent investor call. Your product photography can fuel counterfeit listings. Your visual identity can be replicated with pixel-perfect accuracy and deployed in phishing campaigns that the FBI judges increasingly indistinguishable from the real thing.

This means that **C2PA is not only about transparency but also about cybersecurity.** When every legitimate asset carries a cryptographically signed credential, a verifiable chain of trust is created, from creation to consumption. An asset without this credential has been tampered with or is entirely fake.

The parallel to physical supply chains is instructive. **Two decades ago, manufacturers invested billions in Radio Frequency Identification (RFID) and track-and-trace systems to stop counterfeiting. C2PA is the digital equivalent.** The content supply chain is the manufacturing floor, and any asset without a provenance credential is an untagged product that is unverifiable, and vulnerable.

AI-powered deepfakes drove 30% of high-impact corporate impersonation attacks in 2025, resulting in \$200M+ in losses in Q1 alone



Seven moves for the CMO

01 ***Audit your content ecosystem for provenance readiness.***

Map gaps in your DAM, CMS, and agency workflows. Most strip metadata, don't preserve credentials, or can't distinguish AI from human-created assets. Conducting the gap analysis is itself illuminating.



02 ***Embed C2PA into your marketing technology stack, not around it.***

Adobe has integrated content credentials into its GenStudio and Firefly Services. If you're running an Adobe ecosystem, the capability is already there and just needs to be switched on. If you're migrating platforms, make C2PA compliance a requirement in your RFP, not an afterthought.



03 ***Prepare for the EU AI Act now, not in August 2026.***

Article 50's transparency obligations (machine-readable marking, detection tools, compliance documents) take effect in August 2026. The Code of Practice will be finalised in June 2026. Start building labelling infrastructure today if you produce AI content for European markets.



04 ***Make provenance a brand asset, not just a compliance burden.***

The content credentials icon is designed to be as ubiquitous as the copyright symbol. Early adopters who display it prominently are making a statement: we believe in what we make, and we can prove it. In a market that lacks trust this is not just good governance, but good marketing.



05 ***Engage your implementation and technology partners, experts and advisors.***

Deloitte is in the C2PA coalition, but membership without activation wastes the opportunity. Demand your transformation partners build C2PA compliance into every content supply chain engagement—from DAM to agentic workflows.



06 ***Treat content provenance as a cybersecurity control, not a marketing nice-to-have***

Brief your CISO. Connect brand safety with security ops. With deepfake impersonation attacks hitting 43% of organisations, content credentials strategy belongs in threat intelligence reviews, not marketing silos.



07 ***Build your digital asset forensics capability now***

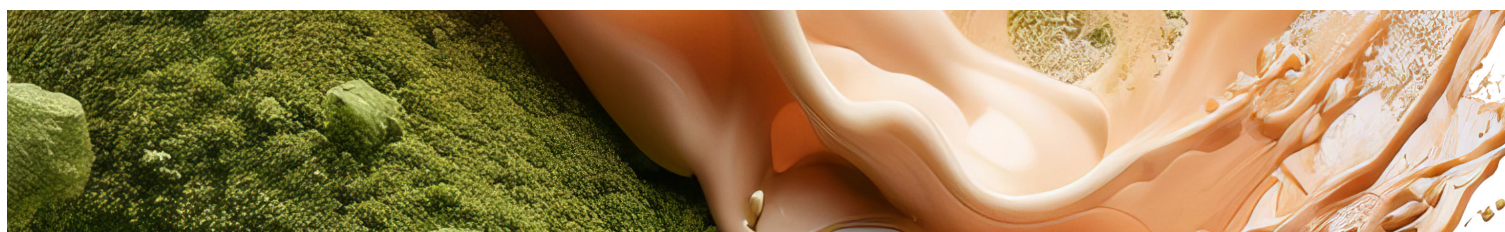
Establish protocols for detecting synthetic content that is misusing your brand. Use C2PA tools to baseline authenticated assets so you can prove provenance and ownership when counterfeits surface.





Sources

1. C2PA & Content Credentials
2. Coalition for Content Provenance and Authenticity (C2PA). c2pa.org
3. Content Authenticity Initiative. "Reflecting on the 2025 Content Authenticity Summit at Cornell Tech." contentauthenticity.org/blog/content-authenticity-summit-2025
4. C2PA. "Introducing Official Content Credentials Icon." spec.c2pa.org/post/contentcredentials
5. C2PA. "Content Credentials White Paper." September 2025. c2pa.org/wp-content/uploads/sites/33/2025/10/content_credentials_wp_0925.pdf
6. World Privacy Forum. "Privacy, Identity and Trust in C2PA: A Technical Review." 2025. worldprivacyforum.org/posts/privacy-identity-and-trust-in-c2pa
7. Trust Over IP. "The C2PA Conformance Program, Scott Perry." July 2025. trustoverip.org/blog/2025/05/20/egwg-2025-05-15-the-c2pa-conformance-program-scott-perry
8. Adobe. "Content Authenticity Arrives for Enterprises." 2025. business.adobe.com/blog/content-authenticity-arrives-for-enterprises
9. Publicis Groupe. "First Holding Company to Join C2PA as Steering Committee Member." June 2023. publicisgroupe.com/en/news/press-releases/publicis-groupe-commits-to-lead-responsible-use-of-artificial-intelligence
10. Wikipedia. "Content Authenticity Initiative." Updated February 2026. en.wikipedia.org/wiki/Content_Authenticity_Initiative
11. Library of Congress. "New Community of Practice for Exploring Content Provenance and Authenticity in the Age of AI." July 2025. blogs.loc.gov/thesignal/2025/07/c2pa-glam
12. EU Regulation & AI Act
13. European Commission. "First Draft Code of Practice on Marking and Labelling of AI-Generated Content." December 2025. digital-strategy.ec.europa.eu/en/library/first-draft-code-practice-transparency-ai-generated-content
14. European Commission. "Code of Practice on Marking and Labelling of AI-Generated Content." digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content
15. ITI. "Tech's Expectations for the EU AI Act Transparency Code of Practice." 2025. itic.org/news-events/techwonk-blog/techs-expectations-for-the-eu-ai-act-transparency-code-of-practice
16. Cooley LLP. "EU AI Act: First Draft Code of Practice on Transparency and Watermarking Released." December 2025. cooley.com/news/insight/2025/2025-12-18-eu-ai-act-first-draft-code-of-practice-on-transparency-and-watermarking-released
17. Cybersecurity & Deepfake Threats
18. Cyble. "Deepfake-as-a-Service Exploded in 2025: 2026 Threats Ahead." December 2025. cyble.com/knowledge-hub/deepfake-as-a-service-exploded-in-2025
19. Cyble. "Brand Impersonation 2025: Major Threats and What's Coming 2026." December 2025. cyble.com/knowledge-hub/brand-impersonation-2025-threats-2026
20. The D&O Diary. "The Growing Threat of AI Deepfake Attacks." August 2025. dandodiary.com/2025/08/articles/cyber-liability/the-growing-threat-of-ai-deepfake-attacks
21. World Economic Forum. "Detecting Dangerous AI Is Essential in the Deepfake Era." July 2025. weforum.org/stories/2025/07/why-detecting-dangerous-ai-is-key-to-keeping-trust-alive
22. Gartner. "Why CIOs Can't Ignore the Rising Tide of Deepfake Attacks." September 2025. gartner.com/en/newsroom/press-releases/2025-09-02-why-cios-cannot-ignore-the-rising-tide-of-deepfake-attacks
23. BlackCloak. "Understanding and Countering Deepfakes in 2025." October 2025. blackcloak.io/the-evolving-executive-threat-understanding-and-countering-deepfakes-in-2025
24. Fortinet. "Deepfake AI and Cybersecurity: Safeguarding Digital Trust in the AI Era." 2025. fortinet.com/resources/cyberglossary/deepfake-ai
25. Wall Street Journal. (n.d.). AI drives rise in CEO impersonator scams, June 2026
26. FBI/IC3 Public Service Announcement, December 2025





Authors

Anne Garcia-Terrero

Senior Manager, Customer Strategist

Email: agarciaterrero@deloitte.ch

Marcin Skucz

Director, Content Supply Chain EMEA Lead

Email: mwskucz@deloitte.ch

Contact us



Cedric Nabe

Partner, Swiss Romandie
Cyber Lead

Email: cnabe@deloitte.ch



Dannie Ivanova

Partner, Global CMO
Program Lead

Email: divanova@deloitte.ch



Marcin Skucz

Director, Content Supply Chain
EMEA Lead

Email: mwskucz@deloitte.ch





This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte AG accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte AG is an affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/ch/about to learn more about our global network of member firms.

Deloitte AG is an audit firm recognised and supervised by the Federal Audit Oversight Authority (FAOA) and the Swiss Financial Market Supervisory Authority (FINMA).

© 2026 Deloitte AG. All rights reserved.