Rapid Response

The EU AI act

Brand responsibility in an era of AI legislation

Updated: March 22nd 2024

Better decisions, faster.

OMD

The world's first AI legislation

EU AI Act adopted

The widespread impact of emerging AI technologies is becoming clearer by the day.

As a general-purpose technology, AI is attracting the attention of legislators worldwide seeking to balance the economic growth potential with multiple possible negative externalities.

To date, the US has utilized Executive Orders to shape future development while India is taking a more laissez-faire approach.

Last week, the European Union parliament passed the Artificial Intelligence Act, the world's first significant legislation to shape the development and use of AI.

As seen with the widespread adoption of GDPR principles, we can expect this act to become the basis for global legislation. According to a recent IAB survey, this global privacy legislation has a measurable effect on ad budgets.

Like GDPR, the AI act has teeth, with fines for non-compliance of up to 35 million Euros or 7% of worldwide annual turnover, whichever is higher.

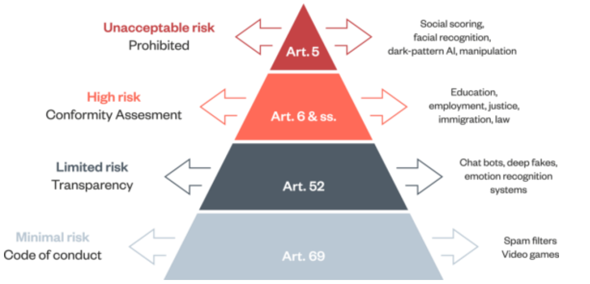
Not only EU businesses should take heed; any business worldwide is impacted if the output produced by their AI systems is used in Europe.

People will have the right to file complaints about AI systems to designated national authorities, who will enforce the AI Act and impose sanctions for violations.

Although final ratification is still required, the AI Act can be expected to become law in Q2 2024. Prohibited systems will be banned within six months, and the act will be fully applicable in just over two years.

Advertisers managing risk

The AI Act follows a risk-based approach, meaning different AI systems are subject to various levels of regulation depending on their potential impact on human rights and safety.


Unacceptable risk
Prohibited
Art. 5
Social scoring, facial recognition, dark-pattern AI, manipulation
High risk
Conformity Assesment
Art. 6 & ss.
Education, employment, justice, immigration, law
Limited risk
Transparency
Art. 52
Chat bots, deep fakes, emotion recognition systems
Minimal risk
Code of conduct
Art. 69
Spam filters
Video games

AI systems that are deemed unacceptable risks are prohibited outright. The act mentions examples such as cognitive behavioral manipulation of people, social scoring, biometric identification, and categorization of people, such as facial recognition.

This may limit some potential use cases of AI technology, such as personal targeting in out of home environments. The act will clarify what profiling and targeting consumers is acceptable, even based on non-PII data.

High-risk AI systems that impact infrastructure, education, safety, public services, and employment must undergo a conformity assessment before being put on the market and throughout their lifecycle.

They must also comply with specific requirements, such as transparency, human oversight, data quality, accuracy, robustness, and cybersecurity.

The AI Act also covers generative AI technologies like chatbots and content creation tools. Each of these systems must disclose that they are not human and respect the intellectual property rights of the data used for training.

The act also sets out principles to prevent bias and discrimination in model training and output. This has been a core focus in Omni's use of AI tools.

Platforms are preparing for this reality. This week, YouTube announced a mechanism for creators to label videos that contain AI-generated content.

Trust and authenticity initiatives

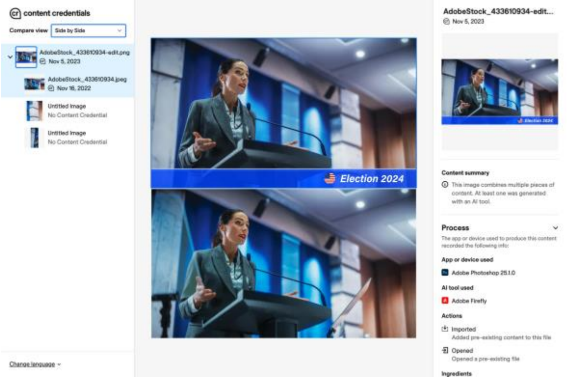
The provenance and authenticity of content have been making headlines worldwide, with the UK Royal Family being caught up in photo manipulation, leading to a frenzy of speculation.

This is within the broader context of:

- Rampant spread of misinformation and disinformation.
- Declining societal trust and negative impact on democratic processes.
- Elections in 60+ countries representing 50% of the global population.
- Brands are fighting MFA websites and programmatic fraud.

Therefore, there is a critical need for transparency and authenticity in content, an ambition that Omnicom has long been committed to.

The Coalition for Content Provenance and Authenticity (C2PA) is a cross-industry initiative that seeks to combat the spread of misleading information online by developing technical standards for certifying the source and history, or provenance, of media content.


content credentials
Compare view: Side by Side
AdobeStock_433610934-edit.png
Nov 5, 2023
AdobeStock_433610934.jpeg
Nov 16, 2022
Untitled Image
No Content Credential
Untitled Image
No Content Credential
Change language

AdobeStock_433610934-edit...
Nov 5, 2023

Content summary
This image combines multiple pieces of content. At least one was generated with an AI tool.

Process
The app or device used to produce this content recorded the following info:
App or device used
Adobe Photoshop 25.1.0
AI tool used
Adobe Firefly
Actions
Imported
Added pre-existing content to this file
Opened
Opened a pre-existing file
Ingredients

C2PA aligns the efforts of Project Origin, a Microsoft- and BBC-led initiative that tackles disinformation in the digital news ecosystem, and the Adobe-led Content Authenticity Initiative (CAI), of which Omnicom was the first advertising holding company to join.

CAI is growing to include Google, Meta, and OpenAI as well as Hardware makers, news organizations, and creative products enabling open, secure, and accountable content credentials.

For more information on Omnicom and C2PA/ CAI, email Greg Brown at DAS.

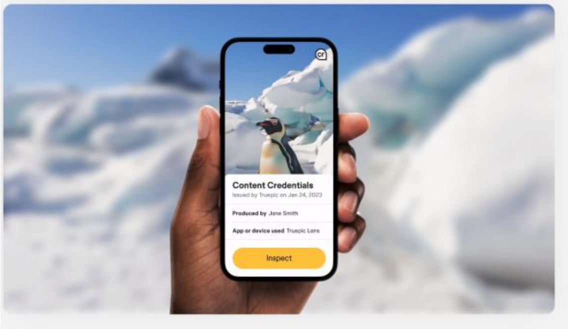
Implications for brands

These initiatives and standards can help ensure the authenticity and credibility of advertising content across channels.

Risks will only increase as content generation and manipulation tools get more sophisticated.

Brands should adopt Content Credentials to mitigate the risks of misinformation, disinformation, and reputational harm. This will future-proof businesses and brands, building an infrastructure of transparency and authenticity.

The EU AI Act illustrates the need to address potential regulatory measures regarding content and watermarks proactively. We can expect to see many more regulations in jurisdictions around the world.


Content Credentials
Issued by Truepic on Jan 24, 2023
Produced by Jane Smith
App or device used Truepic Lens
Inspect

While the authenticity of the products has always been a critical pillar of brands, the authenticity of content and intent are increasingly foundational. Initiatives such as C2PA standards/Content Credentials are essential in an era of plummeting trust.

Brands and agencies should embrace Content Credentials and the C2PA to deliver a competitive advantage in a changing legislative environment.

This is to mitigate risk and build trust as AI services become more sophisticated and deliver an ever-greater impact on our daily lives.

Jean-Paul Edwards
OMD Worldwide Managing Director, Product
jean-paul.edwards@omd.com