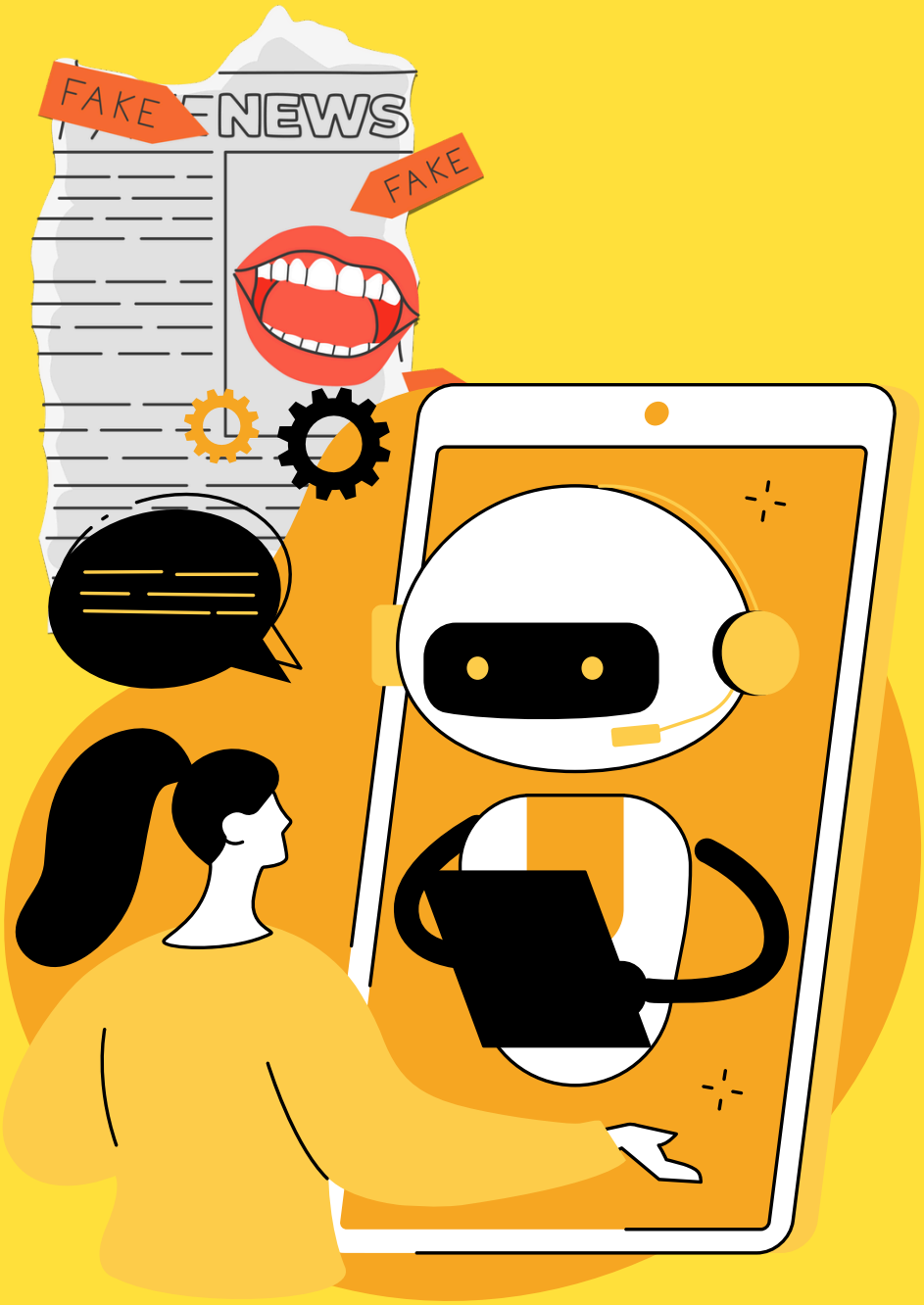
C2PA IN INDIA: UNDERSTANDING IT'S ROLE, LEGAL IMPLICATIONS, AND BUSINESS ADOPTION, 2025



EWA CENTRE
ऐवा सेंटर
डिजिटल भारत के लिए
डिजिटल सहयोग
ContentLens

ACKNOWLEDGEMENTS

Authors: Dhruv Suri, Dylan Sharma from PSA, Legal Counsellors

Advisor: Rohan Sahu, Founder and CEO at ContentLens (www.contentlens.ai)

Design: Tanushree Bhanot

EWA Centre
C-56, Jangpura Extension
New Delhi – 110014, India

EWA Centre is a New Delhi-based tech policy think tank dedicated to bridging the information gap between policymakers, innovators, and users. Our mission is to provide comprehensive research and analysis to inform effective policy decisions that align with technological advancements and societal values.
For more information, please visit www.epwa.in/ewa-centre/.

TABLE OF CONTENTS

1. Executive Summary

In today's digital age, misinformation and content manipulation have become global challenges, exacerbated by advancements in technology. In India, with its vast and diverse digital ecosystem, the spread of fake news, deepfakes, and altered media has grown exponentially. AI-generated misinformation and disinformation are considered to have become the 2nd biggest risk globally and the top risk in India in 2024.[1] This has led to an urgent need for reliable mechanisms that can certify the authenticity and provenance of digital content, ensuring that users have the means to decide whether to trust the media they consume. It is important to remember that the Coalition for Content Provenance and Authenticity (C2PA) does not make a trust decision for the user. It simply provides relevant information to enable the user to decide on what is authentic and safe to view.

The C2PA is a global initiative developed by industry leaders like Adobe, Microsoft, and Intel. Over time, large market leaders like Google, Amazon, Sony, BBC, Meta, TikTok, Nikon, Canon, Fujifilm, and Logitech became members with a common global and industry-agnostic goal to support C2PA and incorporate content credentials.

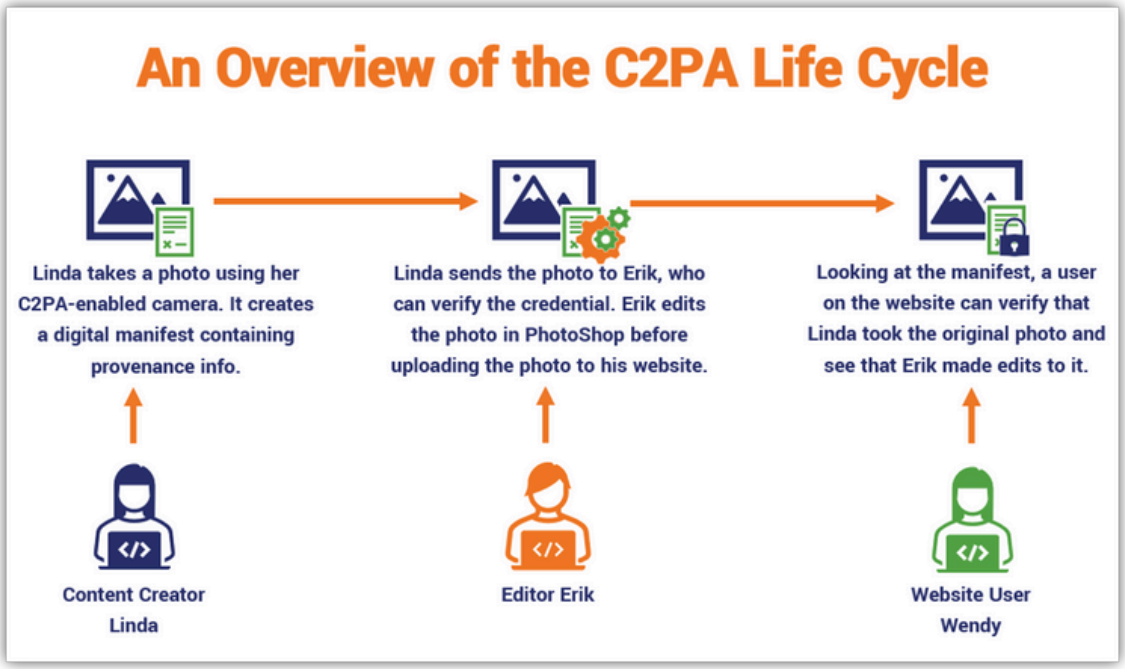


Image No.1- C2PA Life Cycle

1. World Economic Forum, The Global Risk Report 2024 -19th Edition- Insight Report, January 2024, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

C2PA seeks to create a standard for certifying the origin, authenticity, and manipulation of digital content using cryptographically secure metadata attached to media files. Cryptographically secured metadata is additional information about provenance or history of creation, ownership, and usage rights embedded within or associated with media files such as images, audio, and video.[2] This is crucial in communicating the verifiability and authenticity of the media file to help stakeholders make a trust decision.

This white paper explores the implications of C2PA for India, analyzing its potential legal ramifications, applications for businesses, and how it can be integrated into industries ranging from media to e-commerce. This paper also addresses how C2PA can benefit specific groups such as online gamers, influencers, and social media stars while having a broader impact on the general public by reducing the spread of misinformation. Given the rising challenges of content manipulation, introducing C2PA in India could be a pivotal step towards a more secure, transparent, and reliable digital landscape. However, the adoption of such a standard will require awareness, legal alignment, and the active involvement of both private sector stakeholders and the government including the active participation of leading tech companies.

2. Introduction: The Need for Content Provenance in the Digital Era

2.1 Context of Media Misinformation in India

India has become one of the largest internet markets in the world, with over 700 million internet users by the end of December 2022.[3] The rise of social media platforms like WhatsApp, Facebook, and Twitter has contributed significantly to India's digital engagement. However, this growth has also exposed the population to increased misinformation, manipulated content, and digital fraud. The widespread circulation of fake news, altered images, and deepfake videos has become a critical challenge, affecting political discourse, public health campaigns, and consumer behaviour. During the COVID-19 pandemic, misinformation about health and vaccination spread quickly, resulting in confusion and mistrust among the public.

2. Eoghan Casey, Curtis W. Rose, Handbook of Digital Forensics and Investigation, 2010, https://www.sciencedirect.com/topics/computer-science/embedded-metadata

3. Javed Farooqui, Report says over 700 million active internet users in India as of December 2022, The Economic Times, March 2023, https://economictimes.indiatimes.com/tech/technology/report-says-over-700-million-active-internet-users-in-india-as-of-december-2022/articleshow/98673654.cms

4. Abhinav Gupta & Pratyush Ranjan, PTI Fact Check: Fake video of Bill Gates' interview peddled as real on social media; Details inside, March 2023, https://www.ptinews.com/fact-detail/Fake-video-of-Bill-Gates%E2%80%99-interview-peddled-as-real-on-social-media;-Details-inside=/287208

5. Jeremy Hsu, Deepfake politicians may have a big influence on India's elections, New Scientist, April 2024, https://www.newscientist.com/article/2427842-deepfake-politicians-may-have-a-big-influence-on-indias-elections/

A video went viral in 2023 of Microsoft co-founder Bill Gates being interviewed by an Australian journalist and accused of profiting from the sale of "unapproved COVID-19 vaccines". The Press Trust of India confirmed this was a deepfake video, i.e., the audio was AI-generated.[4] Similarly, political campaigns have seen a rise in doctored images and videos aimed at influencing public opinion. Political campaigns in the 2024 general elections were using AI-generated content such as deepfakes of politicians to sway voters.[5] A rather harmless instance is a video on WhatsApp featuring an AI-generated avatar of PM Modi addressing voters by name.[6] However, in contrast, fake videos have been going viral of actors Aamir Khan and Ranveer Singh allegedly making anti-Modi comments before the videos end with pro-Congress slogans.[7] An AI-created video circulated online in November 2024 of Finance Minister Nirmala Sitharaman and RBI Governor Shaktikanta Das promoting an investment application which purportedly allows users to quadruple their investment, and reassuring about its safety.[8]

Popular instances showcasing consequential reputational harm include a deepfake video inappropriately depicting actress Rashmika Mandana where her face was superimposed on the body of a social media influencer,[9] and fabricated videos of the National Stock Exchange MD and CEO Ashishkumar Chauhan making investments and providing tips and advice on investing.[10] Some have also led to mammoth financial losses, such as the Hong Kong (Arup) deepfake scam where an employee in the finance team of a large British multinational design and engineering company Arup was duped into attending a video call with people he believed were the chief financial officer and other members of staff. The fraudsters used the faces and voices of his colleagues and directed him to send $25.6 million.[11] Worse still, in 2023, a group of scamsters used deepfake technology to look like attractive women, message and develop romantic relations with unsuspecting men in Hong Kong, Singapore, India and China, and manipulate them into providing funds for bogus crypto investments only to flee with the money, costing the victims a total of $46 million.[12] The Indian Government has taken cognizance of the issue and taken action to protect the general public. For instance, in 2021, the Ministry of Electronics and Information Technology (MeitY) notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 whereunder intermediaries such as search engines, online payment sites, online marketplaces, and those providing telecom, network, and internet services are required to, as part of due diligence, implement measures to ensure no patently false, misleading or deceptive information is published and shared.[13]

6. id

7. Aditya Kalra, Munsif Vengattil and Dhwani Pandya, Deepfakes of Bollywood stars spark worries of AI meddling in India election, Reuters, April 2024, https://www.reuters.com/world/india/deepfakes-bollywood-stars-spark-worries-ai-meddling-india-election-2024-04-22/

8. Aishwarya Varma, Clip of Nirmala Sitharaman, RBI Governor Promoting Investment App Is a Deepfake, The Quint, November 2024, https://www.thequint.com/news/webqoof/deepfake-of-nirmala-sitharaman-shaktikanta-das-promoting-investment-app-fact-check#read-more#read-more

9. BS Web Team, Rashmika Mandanna's deepfake video goes viral, IT Minister issues warning, November 2023, https://www.business-standard.com/entertainment/rashmika-mandanna-s-deepfake-video-goes-viral-it-minister-issues-warning-123110600940_1.html

In December 2023, MeitY issued an advisory to intermediaries in light of "growing concerns around misinformation powered by AI - Deepfakes"[14] highlighting that the said requirement under the IT Rules aims to "ensure platforms identify and promptly remove misinformation, false or misleading content, and material impersonating others, including deepfakes."[15] It reiterates that users must be informed clearly and precisely about any misleading and untrue content shared or uploaded onto the intermediary platform. This was followed by an additional advisory in March 2024 whereunder the government required intermediaries that permit or facilitate "synthetic creation, generation or modification of a text, audio, visual or audio-visual information...used as misinformation or deepfake" to label or embed such information with a "permanent unique metadata or identifier" used to identify that it has been "created, generated or modified using the computer resource of the intermediary." If any changes are made by a user, the metadata should be "configured to enable identification of such user or computer resource that has effected such change."[16] This is especially important given that in November 2024, the government informed the Delhi High Court that it was actively taking measures to address the deepfake issue and the misuse of technology and that MeitY had set up a committee to deal with this.[17]

In this landscape, a solution that can certify the authenticity and provenance of digital content is essential for platforms to be legally compliant and to instil confidence and trust in their respective users.

2.2 Introduction to C2PA

C2PA was formed in February 2021[18] to tackle precisely these kinds of challenges. It is a cross-industry effort by technology and media companies aimed at developing open standards to provide a mechanism for verifying the authenticity of digital content. It unifies two significant efforts: the Adobe-led Content Authenticity Initiative **(CAI)** which focuses on developing open-source tools that record context and history for digital media, and Project Origin,[19] a collaborative effort led by Microsoft and the British Broadcasting Corporation that creates verification methods of tagging media files with traceable information, enabling viewers to verify the source of the content and detect if and how the content has been modified since initial publication.

10. Press Trust of India, NSE warns investors against deepfake clips of its chief recommending stocks, June 2024, https://www.business-standard.com/markets/news/nse-warns-investors-against-deepfake-clips-of-its-chief-recommending-stocks-124061000836_1.html

11. Kathleen Magramo, British engineering giant Arup revealed as $25 million deepfake scam victim, May 2024, https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html

12. FP Explainers, How deepfake romance scammers stole $46 million from men in India, China, Singapore", October 2024, https://www.firstpost.com/explainers/how-deepfake-romance-scammers-stole-46-million-from-men-in-india-china-singapore-13825760.html

At its core, C2PA aims to create a secure and transparent system that attaches verifiable metadata to images, videos, and audio files, ensuring that anyone interacting with this media can trust its origin. The metadata, often described as a "provenance chain"[20] includes information about the content's creation, editing, and publishing, which can be traced back to the source. It also allows creators to outline how others can use their data for AI training, editing, etc. This, in conjunction with durable content credentials, helps retrace unauthorized versions to the creator's original version.

2.3 Global Push for Content Provenance

On a global scale, the spread of manipulated content has become a growing concern for governments, media outlets, and private organizations. Major incidents of manipulated content in politics, journalism, and business, some of which gravely degrade reputation, have sparked conversations on the need for robust systems of authentication. In May 2023, a doctored video emerged on Facebook of US President Joe Biden touching his granddaughter inappropriately, with the caption calling him a paedophile.[21] Governments in the United States of America[22] and European nations[23] are actively working on regulatory frameworks to combat misinformation.

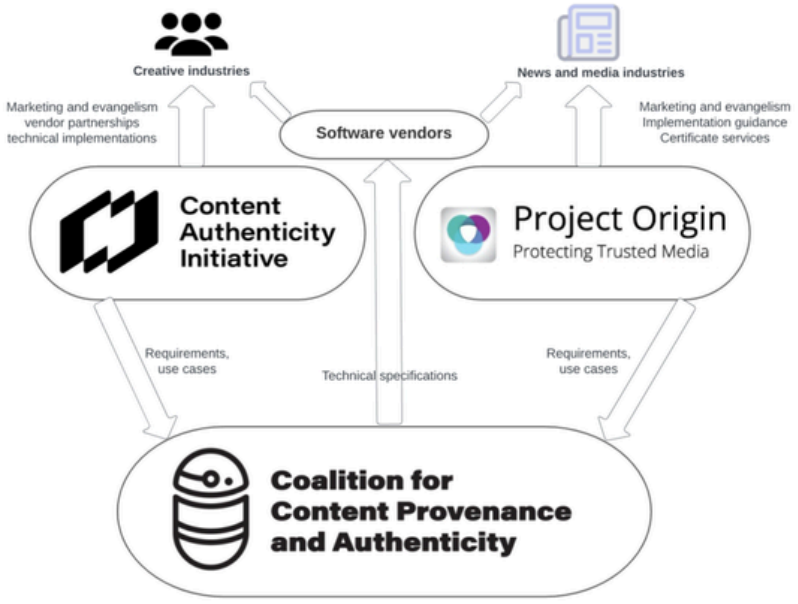


Image No.2- Overview of the C2PA trust ecosystem, showing how the C2PA project implements requirements set by both the Content Authenticity Initiative and Project Origin.

13. Rule 3(1)(b)(v) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

14. PIB Delhi, MeitY issues advisory to all intermediaries to comply with existing IT rules, December 2023, http://bit.ly/49Zzz6d

15. id

16. Advisory No. eNo. 2(4)/2023-CyberLaws-3 dated March 2024 issued by MeitY, Government of India, Cyber Law and Data Governance Group

The European Parliament published a research report[24] in December 2023 noting that the former US President Joe Biden signed an executive order[25] in October 2023 requiring the US Administration to develop effective labelling and content provenance mechanisms. Hence, people can determine when content is generated using AI, thereby reducing the risks posed by synthetic AI-generated content. The report also noted that the G7 had adopted the International Guiding Principles on AI in October 2023, recommending that organizations developing and using advanced AI systems should develop and deploy reliable content authentication and provenance mechanisms including watermarking to enable users to identify AI-generated content.

Members of the US government introduced a bill in July 2024 called the Content Origin Protection and Integrity from Edited and Deepfaked Media Act.[26] While not yet enacted, it will be an important step towards promoting transparency of content and content provenance information. One key issue the bill intends to address is that "it is becoming increasingly difficult to assess the nature, origins, and authenticity of digital content."[27]

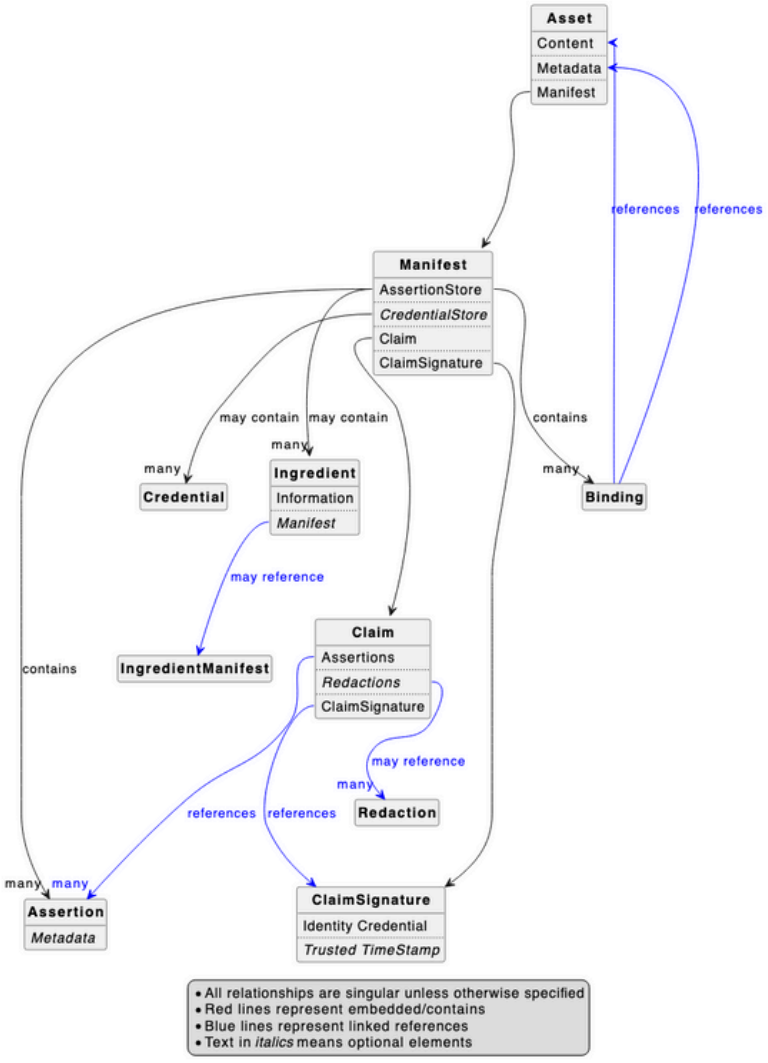


Image No.3- C2PA Entity Diagram

It also proposes certain relevant solutions - (a) create standards for content provenance information technologies and the detection of artificially generated and modified content, (b) enable provenance information to be added when tools are used for artificial creation or modification of content, and (c) illegalize the intentional removal, alteration or tampering of provenance information.

California passed the California AI Transparency Act in September 2024 to govern the development of standards and technologies to determine digital content provenance.[28] The law specifically provides that, effective January 1, 2026, persons or organizations that code or create generative AI systems must include a latent disclosure in AI-generated image, video, or audio content created by the system that conveys information about the provenance of the content. Failure to comply will result in a penalty of $5,000 per violation. Around the same time, California also passed the law on AI Training Data Transparency, mandating that, for generative AI systems or services released on or after January 1, 2022, and made publicly available, the developer must post, on his website, documentation regarding the data used to train the system including a summary of the datasets used in its development.[29] This includes the source or owners of the data, a description of how the datasets further the intended purpose of the system, whether the datasets include any data protected by copyright, trademark, or patent, or whether the datasets are entirely in the public domain, whether the datasets were purchased or licensed by the developer, whether the datasets include personal information, and whether there was any modification made to the original datasets by the developer.

The EU is another major power working to combat the issue of misinformation, especially in the form of deepfakes. In 2024, the EU passed the Artificial Intelligence Act, 2024 as a legal framework governing the development and use of AI systems in a "human-centric and trustworthy"[30] manner. The act recognizes that increasing amounts of AI-generated content are making it difficult to distinguish between human-generated authentic and artificial work. This affects the "integrity and trust in the information ecosystem"[31] with threats of misinformation and deception. Therefore, the act mandates that providers of AI systems embed technology for marking the output in a machine-readable format to identify that it has been created or manipulated by AI. Some methods proposed are watermarks, metadata identifications, and cryptographic methods for proving provenance and authenticity, etc.

17. Press Trust of India, HC directs Centre to nominate panel members to examine deepfake menace, November 2024, https://www.ptinews.com/story/national/hc-directs-centre-to-nominate-panel-members-to-examine-deepfake-menace/2009006

18. FAQ - C2PA, https://c2pa.org/faq/#:~:text=The%20C2PA%20was%20founded%20February,BBC%2C%20Intel%2C%20and%20Truepic.

19. Overview - Project Origin, https://www.originproject.info/about

20. The record of ownership or history of an item throughout its lifecycle, starting from the original source to each stage of documented history

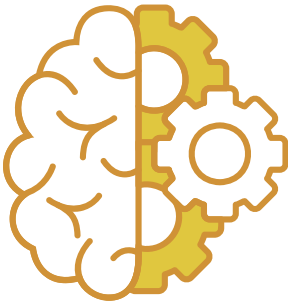
The United Nations General Assembly (**UNGA**) adopted a Resolution in March 2024 on AI systems for sustainable development, encouraging its Member States like the UK, USA, Japan, Canada, Singapore, etc. to promote safe, secure and trustworthy AI systems for the benefit of all and to foster an enabling environment for such systems to address global challenges, including achieving economic, social, and environmental sustainable development.[32] One major recommendation is to develop and deploy effective, accessible, adaptable, internationally interoperable technical tools, standards or practices, including reliable content authentication and provenance mechanisms such as watermarking or labelling, thereby enabling users to identify information manipulation, distinguish or determine the origins of authentic digital content and AI-generated or manipulated digital content, and consequently increasing media and information literacy.

However, these laws, requirements, and recommendations can only effectively mitigate the threats and protect the average consumer of information online when businesses develop and adopt a strong technical ecosystem for detection, disclosure, and identification. C2PA is part of this larger ecosystem. India, with its dynamic and fast-paced digital landscape, stands at a critical juncture. Given its global role as an IT and digital hub, adopting standards like C2PA could help India lead in promoting media transparency and authenticity.

3. Understanding C2PA: The Technology and Framework

3.1 Definition and Overview

C2PA aims to establish an open technical standard that can help identify the origin and history of digital media. By embedding cryptographic secure metadata directly into digital files, C2PA provides a verifiable "chain of provenance" that documents information regarding the origin and history of the content piece, from its creation to the present, almost like a description of where it came from and what happened to it along the way including if any changes were made along the way. In the artistic context, this is the history of the artwork including who created it, who owned it, where it has been displayed, etc.



21. Vittoria Elliott, A Doctored Biden Video Is a Test Case for Facebook's Deepfake Policies, WIRED, October 2023 https://www.wired.com/story/a-doctored-biden-video-is-a-test-case-for-facebooks-deepfake-policies/

22. Some laws in the United States dealing with deepfakes and misleading content include the Malicious Deep Fake Prohibition Act of 2018, Deepfakes Accountability Act of 2020, The National Defence Authorization Act of 2021, The Computer Fraud and Abuse Act of 1986, California Assembly Bill No. 730 of 2019 and Assembly Bill No. 2839 of 2024, and Virginia Code sections 18.2-386.2 of 2020

23. Some laws in the EU dealing with deepfakes and misleading content include the Digital Services Act of 2022, the European Union Artificial Intelligence Act of 2024 (to be enacted), and The Code of Practice on Disinformation of 2022

In digital data, provenance tracks the origins and changes made to the data. C2PA does not give definitive views on whether to view content or not, but provides the means to verify the source, origin and history, enabling the user to make an informed decision on whether to trust the veracity of the content. This can help media platforms prevent fake content from going live, disincentive unverifiable/suspicious content and provide greater value for authentic and verifiable content.

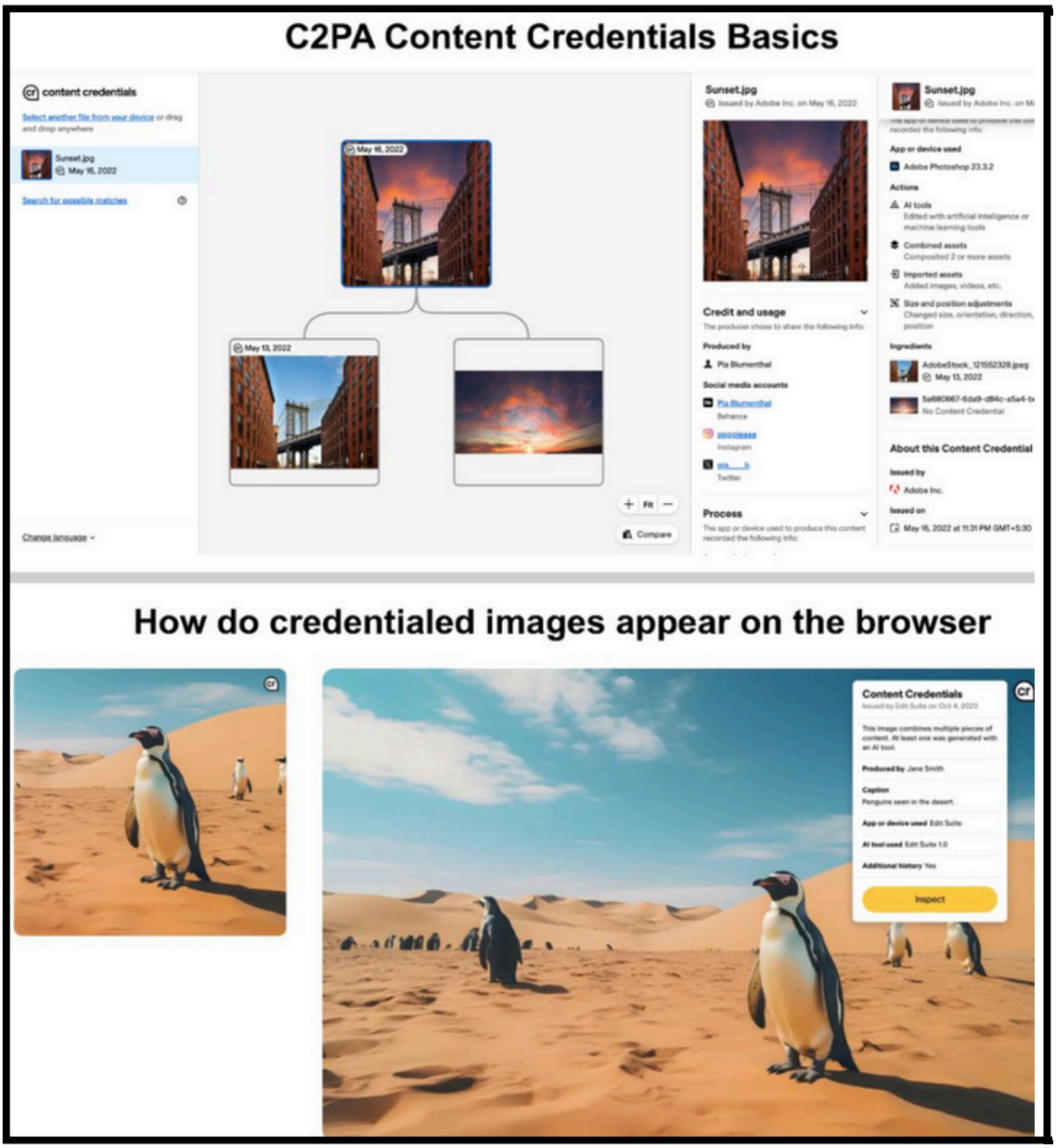


Image No.4- C2PA Content Credentials Basics

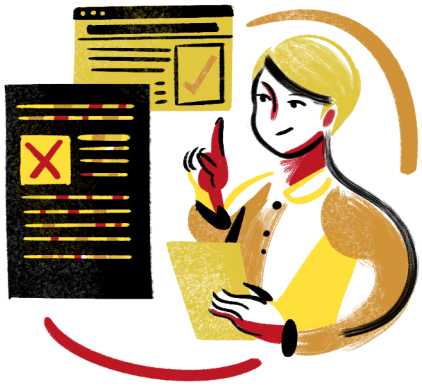
24. European Parliamentary Research Service, Generative AI and watermarking, December 2023 https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI(2023)757583_EN.pdf

25. Joseph R. Biden Jr., Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI, White House, October 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

26. 118th Congress 2D Session, Content Origin Protection and Integrity from Edited and Deepfaked Media Act of 2024, https://www.documentcloud.org/documents/24804105-copied-act?responsive=1&title=1

Every piece of content contains metadata such as creator information, whether it is AI-generated, editing history, technical details including AI tools used to manipulate the content, and ownership verification. However, considering general criticism that metadata or an invisible watermark to label AI-generated content is not sufficient, C2PA creates durable Content Credentials, whereby three techniques used to inform consumers - secure metadata, watermarking (embedding small amounts of information in content undetectable by humans, and that can be decoded using a watermark detector), and fingerprinting (creating a unique code based on pixels, frames, or audio waveforms that can be computed and matched against other instances of the same content with minor alterations) - are combined into a single approach to make them more robust and secure. In this approach, the content is first watermarked and then, a fingerprint of the media form is generated. Both of these are added to the Content Credential which already includes metadata regarding its provenance. The combined result is digitally signed, creating a durable Content Credential.

3.2 Working of C2PA



Envision this - a person takes a photograph on their phone, uploads it to a digital photo editing software to resize and adjust brightness and saturation, and then uploads it on a social media platform. Provided the phone, software, and platform are C2PA-enabled, each will embed specific details like the location where the photo was taken, the make and model of the phone, changes and edits made, the software used, date and time when each change was made, etc. These details will be visible on the social media platform to viewers, allowing them to check the origin and history of changes. The changes could be minor aesthetic edits, or AI morphing of a person, object, animal, etc., all of which will inform viewers whether they are seeing the image as it was originally taken or whether the image is drastically different from the original.

Each piece of information which comprises the provenance of the image is called an assertion. A collection of assertions bundled together form the claim which is digitally signed. All this together forms the C2PA Manifest, embedded into the output image. The Manifest is also stored remotely on the cloud linked by the content's watermark and/or fingerprint. This is known as soft-binding of Manifest, which ensures provenance data can be retrieved even if the embedded C2PA metadata is intentionally or unintentionally stripped off. Importantly, the content creator gets to choose what assertions to include.[33] A major challenge is that every device, tool, and software used must be C2PA-enabled.

Otherwise, provenance data will not be complete since, for instance, non-C2PA-enabled software would not update provenance to reflect edits made on it. However, as global awareness backed by large organizations translates to larger adoption, the chances of the provenance chain breaking will reduce. The C2PA initiative involves several key technology and media companies, including Adobe, Microsoft, Intel, Google, Meta, Sony, TikTok, LinkedIn, BBC, Canon, Nikon, Logitech, OpenAI, ARM, and Truepic. These companies are working to develop a unified system that can be adopted globally, including in India.

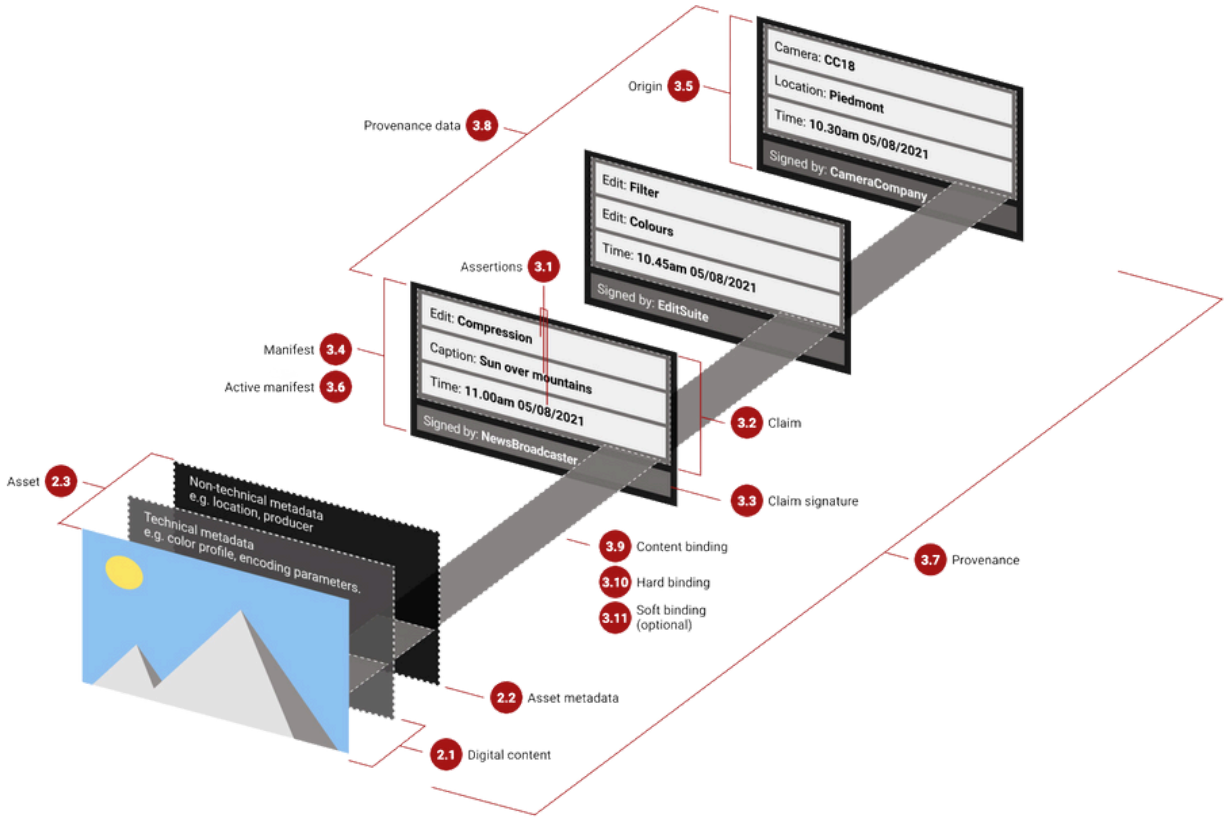


Image No.5- Elements of C2PA

4. The Role of C2PA in Business: How Can Companies Incorporate It?

C2PA is designed primarily for platforms, such as gaming companies or content creation tools, to integrate into their workflows and enable content authentication. However, its benefits extend to end users, including gamers, by ensuring they interact with secure, verified digital content.

C2PA operates as a framework and standard, not as standalone software. Companies adopt it by integrating C2PA-compliant tools or APIs into their existing software development pipelines. This involves embedding cryptographic metadata into digital content during its creation or distribution. For gaming companies, this could mean updating game development workflows to attach C2PA metadata to gameplay files, virtual assets, or in-game recordings.

Gaming platforms typically partner with third-party providers who offer C2PA implementation tools, or they develop in-house solutions based on the open standards published by the Coalition for Content Provenance and Authenticity. These tools ensure compliance with the standard, which includes generating secure provenance data, embedding cryptographic signatures, and maintaining compatibility with existing systems. It works in the following way:

- **Provenance Metadata Generation:** C2PA-compliant tools generate metadata such as creator identity, editing history, and authenticity markers.
- **Embedding Metadata:** The metadata is cryptographically embedded in the content itself (e.g., gameplay footage or virtual items).
- **Verification Tools:** Platforms use verification APIs or interfaces, allowing end users to confirm the authenticity of content.

Adoption also requires compliance with privacy and security guidelines, particularly in India where regulations like the Digital Personal Data Protection Act could influence metadata handling. For most companies, licensing and integrating C2PA-compliant software tools is the most practical route, avoiding the need for in-house development.

4.1 Media and News Organizations

Media companies, publishing houses, and digital platforms have to mandate that C2PA metadata is embedded into all videos, images, articles, and other digital assets uploaded, shared, or promoted through their websites and platforms. This will ensure that all content accessed by viewers is verifiable.

27. *id.* Section 2(2)
28. Senate Bill No. 942, Chapter 291, approved and chaptered on September 2024
29. Assembly Bill No. 2013, Chapter 817, approved and chaptered on September 2024
30. Recital 1, Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 2024, Official Journal of the EU
31. id. Recital 133

4.1.1 BBC Case Study

The BBC founded, developed, and actively pushed for the adoption of C2PA. The company explained how C2PA can be used by media companies;[34] An image is captured by a photographer who then uploads the picture from their camera to their computer for some edits such as increasing brightness or correcting white balance. They may then send the edited image to an agency which will catalogue the image and information about where and when it was captured, a description, etc. The agency might also edit the image by cropping or resizing. If the BBC decides to use that photo, it will make further edits before releasing it to the public as part of a news article. All these edits need to be individually signed, after which, they get added to the provenance chain, allowing these to be viewed back to the point at which the camera took the photo. Each edit, signed by the entity that made them, can then let the user know what edit was performed. The spec also allows for thumbnails at each step to be recorded. Therefore, every image and video uploaded on the platform will have Content Credentials that provide the user with a brief description of the image, when it was posted, who created it, where it was created, and a list of edits made. This is essential to enable viewers to trace where the content originated, confirming that it hasn't been doctored, and confirming the sources. BBC has published some images and videos with C2PA-embedded metadata showing the fact-checking process that has been undertaken.

4.1.2 LinkedIn Case Study

LinkedIn adopted the C2PA standard in May 2024. Content, including AI-generated images, videos, and posts, containing C2PA metadata and uploaded on the platform is automatically labelled with a "Cr" icon. Clicking on the icon allows the user to view the Content Credentials about the source and history of the media. This includes whether the image is AI-generated and the date of creation. At present, this feature is restricted to the LinkedIn feed, but the company intends to extend coverage to ads on the platform. The primary goal is to provide a verifiable trail of where the content originated from and whether it was edited, to help keep digital information reliable, protect against unauthorised use, and create a transparent, secure digital environment for creators, publishers, and members.[35]

32. UNGA Resolution No. A/78/L.49, Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development, March 2024, https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf

33. C2PA Explainer version 1.3, Chapter 3 - Fundamentals (FAQs), October 2023, https://c2pa.org/specifications/specifications/1.3/explainer/_attachments/Explainer.pdf

34. Charlie Halford, Mark the good stuff: Content provenance and the fight against disinformation, BBC Research and Development, March 2024, https://www.bbc.co.uk/rd/blog/2024-03-c2pa-verification-news-journalism-credentials

4.1.3 Other Examples

TikTok has adopted a similar mechanism where it detects when images or videos are uploaded to its platform containing metadata tags indicating the presence of AI-generated content and automatically labels these.[36] It also adds tags to content generated using TikTok's AI effects that remain in place even if the content is downloaded for posting elsewhere. A German media processing and distribution company, G&L Systemhaus, integrated C2PA metadata into existing production and publishing processes.[37]Each image and video uploaded onto the platform will be embedded with metadata, validated and signed with a verification seal displayed in the media player. With this, content authenticity can be cryptographically certified and verified throughout its lifecycle.

In India, the media sector plays a critical role in shaping public opinion. People rely greatly on digital and print media and news agencies to educate them about current affairs and global events. Apart from televised broadcasts, most news agencies also publish news pieces and articles on their websites and apps. The issue therefore becomes two-sided. Given the extent of the spread of false and misleading information online, whether written or as images, videos and audio files, media houses and news agencies need to be cautious about their information sources. C2PA can help rebuild public trust by allowing news organizations to prove the authenticity of their reports, images, and videos to combat misinformation and disinformation simply put, it helps track the origin and history of media files allowing them to ensure they publish credible and accurate information. In summary, C2PA empowers media and news organizations by enhancing content integrity, promoting transparency, ensuring copyright protection, and combating the spread of fake news, thereby allowing them to maintain their credibility in an increasingly digital and content-rich world.

4.2 Businesses and E-commerce

In sectors like e-commerce and digital advertising, C2PA can ensure the integrity of product listings, advertisements, and customer reviews. This is crucial in a market where consumers are increasingly wary of manipulated content and fake reviews. C2PA can prevent the listing of counterfeit products where content is copied, edited and listed back on e-commerce platforms.

35. Patrick Corrigan, LinkedIn Adopts C2PA Standard, May 2024, https://www.linkedin.com/pulse/linkedin-adopts-c2pa-standard-patrick-corrigan-kwldf/?trackingId=4gnjmapwRsmugUNqwj0fRw%3D%3D

36. Umar Shakir, TikTok is adding an 'AI-generated' label to watermarked third-party content, The Verge, May 2024, https://www.theverge.com/2024/5/9/24152667/tiktok-ai-generated-label-content-credentials-cai-c2pa

37. Jörn Krieger, G&L enables broadcasters to become C2PA compliant, August 2024, https://www.broadbandtvnews.com/2024/08/27/gl-enables-broadcasters-to-become-c2pa-compliant/

Additionally, the provenance of delivered products can be tracked to reduce fraud, piracy and counterfeiting. Businesses in India can leverage C2PA to establish a new level of transparency and trust with their customers. Incorporating C2PA into a business model offers businesses an opportunity to improve content integrity, enhance brand trust, protect intellectual property, and address growing concerns around misinformation, content manipulation, and copyright infringement.

E-commerce brands and platforms, and online stores and websites can embed C2PA metadata in product images, product descriptions, and customer reviews to authenticate origin. This is especially useful for high-value goods such as luxury items or rare collectables that can be tracked with provenance metadata to ensure buyers are receiving authentic product information. For example, a luxury watch brand website could embed C2PA metadata in its product advertisements to prove authenticity and distinguish it from counterfeit versions of the product listed on other online marketplaces or AI-generated versions of the advertisement improperly depicting the product. Apart from strengthening customer confidence and trust, this helps protect brand reputation and value. The company can prevent the sale of counterfeit goods by ensuring that only verified products are listed or advertised by trusted sources. The company can establish clarity of the origin of the assets associated with the brand.

In 2023, an AI-generated image of Pope Francis wearing a Balenciaga jacket went viral, causing some viewers to believe it was real or that it was a marketing campaign by the brand.[38] Such an image, if unverified, could prove detrimental or controversial for a brand if consumers affected by certain sensitive topics are unable to establish the source and veracity of the image.

4.3 Tech Companies and Service Providers

Depending on the nature of the product and service being provided, C2PA has multifaceted uses. For instance, Cloudinary, an API cloud-based solution that helps automate all processes related to managing images and videos, now supports adding signed provenance metadata in compliance with the C2PA Content Credentials specification on its image and video API platform.[39]In the initial stages, Cloudinary has implemented C2PA to specify whether edits made to images and videos involved substantial altering of the pixels or simply optimized them for delivery while preserving existing content credentials. Sony, recently in 2024, launched firmware updates for some of its cameras which introduced a proprietary in-camera digital signature and C2PA format support.[40] The purpose is to enable users of the camera and news agencies who use the end-product content to validate the authenticity of images. This adoption is part of Sony's efforts to implement technology in its cameras that would help fight against fake and manipulated imagery.

5. C2PA and Online Gaming: Transforming the Indian Gaming Landscape

India has 568 million gamers thereby making it the largest gaming market globally, with the number of Indian gaming companies growing from 25 in 2015 to over 1400 in 2023. With the exponential growth, issues related to authenticity, security, and ownership in the gaming world are bound to arise. For game developers, especially independent ones, C2PA can protect against the content theft and piracy. The C2PA metadata embedded within original game assets including gameplay footage, in-game assets, modifications, or streamed content can be traced back to the developer, ensuring proper ownership and reducing piracy. This will ensure that the game or its elements are not misused or illegally distributed. For instance, a game developer can embed C2PA data into gameplay footage shared on streaming platforms, so if someone posts altered gameplay without credit or permission, the metadata can help trace the origin. This is especially useful to verify in-game purchases such as skins, usable items like weapons, or NFTs. C2PA metadata embedded in such digital assets can provide proof of originality, authenticity, and ownership once purchased. For example, when a gamer purchases a limited edition skin or weapon for Fortnite or Counter-Strike, C2PA could be used to ensure that this item is truly from the official developer and not a counterfeit from third-party sites. Many games allow for user-generated modifications or mods where gamers can create and share new content like custom maps, skins, or gameplay changes. C2PA can ensure that these mods are legitimate and it would give the mod creators control over their work, ensuring proper attribution and preventing unauthorized distribution. For example, a gamer creates a custom mod for a game like Minecraft. By using C2PA, they can prove that the mod is their original creation and prevent others from taking credit or distributing it without permission.

[41]

For gamers who stream on platforms like Twitch or YouTube, C2PA can prove the authenticity of their gameplay footage. This is particularly important when streaming exclusive content or competitive gameplay. A pro gamer streaming an exclusive event could embed C2PA metadata to ensure that their audience knows the gameplay footage is real, unaltered, and from the actual stream. This will help preserve the gamer's brand.

38. James Vincent, The Verge, The swagged-out pope is an AI fake — and an early glimpse of a new reality, March 2023, https://www.theverge.com/2023/3/27/23657927/ai-pope-image-fake-midjourney-computer-generated-aesthetic

39. Eric Portis, Combating Fake Visuals: Cloudinary's New C2PA Standard Implementation, Cloudinary Blog, July 2024, https://cloudinary.com/blog/c2pa-standard-implementation

40. Sony Electronics Asia Pacific Pte. Ltd. Press Release, Sony Electronics Delivers Firmware Updates including C2PA Compliancy as a Next Step to Ensure Authenticity of Images, March 2024, https://www.sony-asia.com/pressrelease?prName=sony-electronics-delivers-firmware-updates-including-c2pa-compliancy-as-a-next-step-to-ensure-authenticity-of-images

5.1 Combatting Cheating and Manipulation in Online Games

Challenges such as cheating, unauthorized modifications, and fraudulent activities undermine the fairness and integrity of online gaming. C2PA can address these issues by enabling gaming companies to embed cryptographic metadata into gameplay recordings, ensuring that any tampering is immediately detectable. Gamers can trust that the matches they participate in or watch are authentic and untampered, fostering confidence in the gaming ecosystem. This technology can also help gaming companies detect and prevent unfair practices, improving the overall gaming experience for players.

5.2 Protecting In-Game Digital Assets

As in-game purchases and virtual goods grow in popularity, ensuring the authenticity of these digital assets is critical. Online gamers are cheated into buying fake in-game boosters, codes, virtual items, and currency, causing large amounts of financial loss.[42] Some common scams include selling nonexistent virtual items or stealing virtual property that has a market value. Cybercriminals use phishing and malware to steal virtual currencies from user accounts. With C2PA, gaming companies can embed secure metadata into virtual items such as skins, weapons, or character upgrades. This ensures players receive verifiably, original items, reducing the risk of counterfeiting and duplication. Additionally, stolen assets can be traced back to their source account. Gamers in India, who often invest significantly in in-game assets, can benefit from this system by being able to confirm the authenticity of their purchases, preventing fraud. This fosters trust between players and game developers, creating a more reliable virtual economy.

5.3 Authenticating Gaming Content and Preventing Fraud

Fraudulent promotional material, manipulated trailers, and phishing scams are common issues faced by gamers in India. Gaming companies can authenticate promotional campaigns, gameplay previews, and influencer collaborations, ensuring gamers can distinguish between genuine and fake content. For instance, a new game launch supported by C2PA-authenticated content would give players confidence that trailers and previews represent the actual game, avoiding deceptive practices. This level of transparency builds trust and encourages players to engage more actively with the gaming community.

41. Interactive Entertainment and Innovative Council and WinZO, India Gaming Report 2024, March 2024, https://www.ieicouncil.org/

42. Emil Eminov and Stephen V. Flowerday, School of Cyber Studies, College of Engineering and Computer Science, The University of Tulsa Suspicious Financial Activity in the Context of In-Game Asset Exchange Marketplace, November 2024, https://doi.org/10.3390/jcp4040043

5.4 Building a Secure and Trusted Gaming Ecosystem

Gaming companies and developers can collaborate with government initiatives promoting digital security and innovation. Incorporating C2PA into their workflows can address the critical issues of cheating, fraud, and content manipulation. Gamers will benefit from a more secure and transparent environment, where they can confidently participate without fear of exploitation or dishonesty. By adopting C2PA, India's online gaming ecosystem can set a new benchmark for trust and authenticity, paving the way for sustainable growth and player satisfaction.

6. Adopting C2PA: A Methodology for Platforms and Users

- **6.1 For Gaming Platforms:**

Companies can start by integrating C2PA-compliant tools into their development pipelines to embed cryptographic metadata into game files, promotional materials, and in-game assets. Partnering with technology providers and leveraging open C2PA standards will help streamline the process.

- **6.2 For Gamers:**

Platforms should educate gamers on how to verify the authenticity of in-game purchases, gameplay data, and communications using C2PA. This could include user-friendly interfaces to check provenance data for content they interact with.

- **6.3 Industry-Wide Pilots:**

Launching pilot projects in collaboration with tech-savvy gamers and communities can help platforms refine their implementation and build trust.

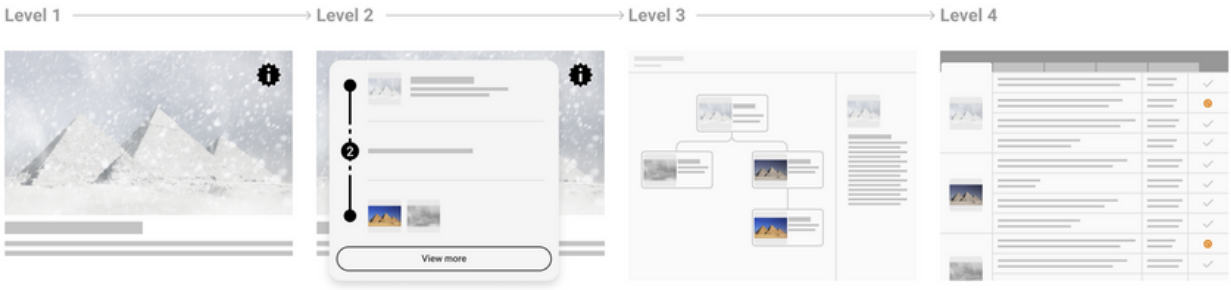
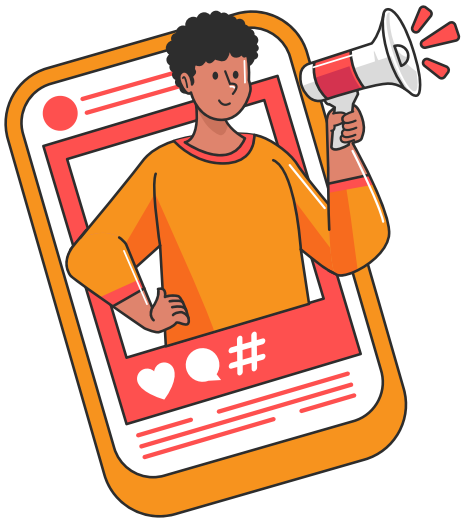


Image No.6- C2PA Disclosure levels

7. C2PA for Social Media Influencers, Creators, and Gamers: Adoption Without Platform Support



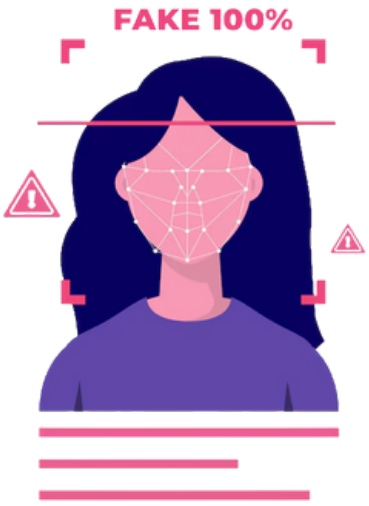
For individual creators like artists, photographers, filmmakers, musicians, and social media influencers, the foremost benefit is increased trust and credibility. Over the last few years, AI-generated content and deepfake videos have become a threat to the reputation, brand image, and character of these creators. For instance, Michel Janse, a social media influencer with almost 150,000 followers on TikTok, discovered a deepfake of herself being used to sell erectile dysfunction drugs.[43] This was offensively different to her usual content of travel, home decor, and wedding planning. Similarly, Jordan Howlett, a creator with 24 million followers on Instagram, TikTok and YouTube, was involved in a deepfake incident mimicking his voice talking about a 7-second ritual to cure blindness and give perfect vision discovered by top researchers from Cambridge.[44] To help combat these attacks and safeguard their credibility, reputation, and brand, C2PA allows creators and influencers to embed metadata to declare their content such as photos, videos, art pieces and posts, is authentic and to outline terms of usage. This enables them to showcase their content as genuine, thereby increasing their credibility and reputation in the industry, and establishing trust with audiences. Digital artists creating and selling NFTs or non-fungible tokens on platforms like OpenSea can use C2PA to authenticate and verify their art by ensuring the piece is linked to its original creator to provide a transparent history of the work, including the creation date, edits made, and any transfer of ownership. This will also enhance trust between the buyer and the artist.

Even without platform-level integration, individual influencers and gamers can adopt C2PA by using tools and workflows that support the standard. C2PA-enabled software—such as video editing tools, image editors, and screen recording applications—allows creators to embed cryptographic provenance metadata directly into their content at the point of creation.

For example, a gamer recording gameplay footage can use a C2PA-compliant screen recording tool to embed metadata documenting the game's date, time, and the hardware used for recording. An influencer editing a promotional video can use a C2PA-enabled editor to embed information such as the creator's identity, the editing software used, and modifications made. The content, when shared on platforms like Instagram or gaming communities, retains its metadata even if the platform does not yet support C2PA.

Verification, in this case, would require external tools or third-party interfaces. Creators can also host verified content externally to overcome platform limitations. For instance, an influencer could provide a link to a third-party repository where followers or collaborators can verify the content's metadata. Gamers could share their verified gameplay files with sponsors or competition organizers directly, bypassing the need for platform-level verification.

8. Fighting Deepfake and Establishing Authenticity



Candidates seeking partnerships with creators and influencers are often cautious about the authenticity of content, especially if they are investing in sponsorships or product placements. Verified content can be more attractive to brands, platforms, or media outlets, and thus, monetization becomes easier for the creator. As audiences become more aware of misleading content online, they are increasingly drawn to creators and influencers who can prove that their content is authentic. For example, an influencer posting a sponsored product review can have C2PA-proven content, showing their followers that the review is genuine and not manipulated or falsified. An influencer's content may be altered in ways that misrepresent the brand they are promoting. The ability to verify that content has not been doctored or falsely presented boosts an influencer's credibility and trustworthiness, thus protecting and bolstering their brand image and values. This also helps maintain the integrity of brand relationships and good relationships with sponsors and companies.

Furthermore, C2PA offers a way to safeguard intellectual property. The provenance data means content creators can prove ownership of their work and track how it's being used or altered. It can also act as a digital signature, ensuring that the influencer's content cannot easily be stolen, repurposed, or manipulated without attribution. This could provide legal protection and make it easier to identify and take action against unauthorized uses. This is particularly important in India, where the digital content industry is multiplying and cases of IP infringement are common. C2PA provenance data injected in the content will safeguard the creator's ownership rights and act as a deterrent for malicious/unauthorized use due to the traceability of the original from fake. For instance, musicians and producers can leverage C2PA to protect their music from piracy and unauthorized remixing.

43. Nitasha Tiku and Pranshu Verma, AI hustlers stole women's faces to put in ads. The law can't help them, The Washington Post, March 2024, https://www.washingtonpost.com/technology/2024/03/28/ai-women-clone-ads/

44. Margi Murphy, How an AI Company Ended Up Fueling Deepfake Audio Boom, Bloomberg, February 2024, https://www.bloomberg.com/news/newsletters/2024-02-21/how-ai-company-elevenlabs-fueled-the-deepfake-audio-boom

Platforms like SoundCloud could integrate C2PA metadata into uploaded tracks to provide proof of ownership and ensure that remixes or covers are properly credited. Similarly, if an influencer's video is shared or reused without permission, the embedded metadata can prove the source.

However, ordinarily, content provenance raises privacy concerns. Metadata about the creator or influencer's name and other personal information, or location may be embedded into the content which creators do not want disclosed. C2PA allows the individual to decide what data is to be included and displayed, thus balancing transparency with privacy rights.

9. Challenges in C2PA Adoption for Individuals

While the mechanism for individual adoption is straightforward, it presents several challenges:

9.1 Verification Accessibility: In the absence of platform integration, verifying C2PA metadata relies on third-party tools. This extra step may discourage casual users or followers from engaging with authenticated content.

9.2 Technical and Financial Barriers: Access to C2PA-enabled software or tools may require licenses or subscriptions, which could be restrictive for small-scale creators or gamers.

9.3 Awareness and Education: Many users—including audiences, brands, and collaborators—might not be familiar with provenance standards or how to verify metadata. Educating stakeholders can be time-consuming and requires consistent communication efforts.

9.4 Lack of Universal Standards: If platforms operate without C2PA support, the absence of a seamless, widely recognized verification process can dilute the impact of embedding provenance metadata.

10. The Future of C2PA in India: Opportunities and Challenges

India presents a massive opportunity for C2PA adoption in the media, entertainment, e-commerce, and journalism sectors. As the world's largest democracy and a hub for technological innovation, India can lead in establishing content authenticity standards for its growing digital population.

The existing Information Technology Act, 2000 and Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 govern the digital space in India. C2PA fits into this framework by providing technological solutions to address content authenticity, aligning with the government's goal to curtail fake news and misinformation. In the coming years, the Indian government plans to enact a new IT legislation called the Digital India Act, 2023 (**DIA**).[45]

The Act, while still under pre-draft consultation, will address online safety and trust, accountability, and new technologies.[46] This is evidence of a progressive IT ecosystem that prioritizes transparency, accountability, innovation and technology, and therefore improves on the existing regulatory landscape that inadequately addresses problems like deepfakes. As governments and regulatory bodies increasingly focus on transparency and accountability in digital media, adopting C2PA standards can help organisations comply with emerging regulatory requirements.

C2PA adoption can also significantly enhance the protection of IP rights. By providing a clear provenance trail for digital content, creators can assert ownership and demonstrate the originality of their work. This is particularly important in industries such as art, music, and literature, where copyright infringement is prevalent. The ability to trace the origin and modifications of digital assets can serve as evidence in legal disputes over IPR. C2PA in IPR protection and enforcement will become increasingly important considering the trend of IP filings has seen positive growth in India over the recent past. In 2022, while global filings for trademarks dropped, India had the 5th highest in volume of trademark filing activity.[47] More filings will probably lead to more infringement claims and disputes. In[48] light of this growth and the government's numerous initiatives and plans since 2020 to strengthen the IPR regime including modernizing IP offices, and digitizing certificates of grant and registration of trademarks, patents and designs,[49] C2PA will prove valuable, especially in the context of digital content. By embedding immutable metadata, C2PA will make it harder for infringers to remove or falsify ownership information. This acts as a deterrent, as the provenance can be verified by anyone interacting with the content. Additionally, the metadata can serve as evidence in legal disputes. Since C2PA relies on cryptographic signatures to verify authenticity, it provides strong proof of ownership, creation date, and modifications, supporting copyright claims. It is also beneficial for media platforms that can use C2PA metadata to automate the detection of infringing content, flagging or removing unauthorized copies before they spread widely. However, there are also some challenges to adoption, as follows -

45. Sanhita Chauriha, VIDHI Centre for Legal Policy, Explained: The Digital India Act 2023, August 8, 2023, https://vidhilegalpolicy.in/blog/explained-the-digital-india-act-2023/

46. Ministry of Electronics and Information Technology, GoI, Proposed Digital India Act, 2023, March 9, 2023, https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

47. World Intellectual Property Organization, World Intellectual Property Indicators 2023, Geneva, https://www.wipo.int/edocs/pubdocs/en/wipo-pub-941-2023-en-world-intellectual-property-indicators-2023.pdf

10.1 Data Privacy Concerns: The government enacted the Digital Personal Data Protection Act (**DPDPA**) to address mounting data privacy issues associated with the increasing reliance on voluminous and diverse collections of data collected, analyzed, and processed to study, control and eventually dictate market conditions, pricing, and purchase trends. Its primary focus is to regulate how personal data,[50] i.e., related to an individual and by which they can be identified, is collected and processed. While the DPDPA does not detail procedural requirements, subsequent Rules will specify how data needs to be collected and stored. The implementation of C2PA could raise concerns about how metadata is collected and handled, particularly since it involves the personal data of creators and publishers including name and location. Although creators can choose what data may be in the provenance chain and redact[51] identifying information, unless C2PA technical specifications and standards include alignment with privacy requirements, it could face pushback from stakeholders.

10.2 Intellectual Property Issues: The provenance chain includes information about ownership of content such as the name of the creator. This could contradict copyright claims or licensing agreements, leading to disputes. For instance, a photographer working for an agency agrees that every photo he clicks at a fashion event shall be the IP of the agency. However, the C2PA-enabled camera he uses will reflect his name as a creator without any mention of the agency, and this could cause misunderstandings regarding ownership of the image.

10.3 Awareness and Acceptance: Given that the concept of content provenance is nascent in India, legal adoption will not guarantee practical implementation. Companies and consumers may not fully understand the importance and functionality of C2PA technology and lack awareness of C2PA's capabilities, which will create scepticism about the need to adopt it.

10.4 Cost for SMEs: Small and medium enterprises (SMEs) may face technical and financial hurdles in adopting the standard. Implementing C2PA requires significant investment in technology and infrastructure, and organizations may need to upgrade their existing systems or develop new ones capable of handling the complex metadata formats C2PA employs. Additionally, organisations may need to invest in training staff or hiring personnel with relevant expertise in metadata management.

48. Economic and Political Weekly - Engage, Scope for Reformative Dispute Resolution in India: Abolition of The Intellectual Property Appellate Board to Arbitration of Intellectual Property Disputes, February 9, 2024, https://www.epw.in/engage/article/scope-reformative-dispute-resolution-india

49. International Trade Administration, Department of Commerce USA, India - Country Commercial Guide: Protecting Intellectual Property, January 12, 2024, https://www.trade.gov/country-commercial-guides/india-protecting-intellectual-property

11. Recommendations for Implementation and Adoption

11.1 Awareness Campaigns

A national awareness campaign led by industry bodies and the government could help Indian companies and consumers understand the benefits of adopting C2PA. Engaging with tech giants and media outlets will also help drive adoption.

11.2 Government Support

Public-private partnerships could be key in promoting C2PA adoption, with government incentives for businesses implementing the standard. Government support by fostering a robust ecosystem for content provenance and authenticity can significantly accelerate adoption. This includes establishing legal frameworks that recognize C2PA metadata as valid evidence of ownership. Subsidies or incentives for media companies, startups, and digital platforms to implement C2PA standards would encourage widespread adoption. Additionally, government-led awareness campaigns can drive education around the importance of provenance and digital integrity. Integrating C2PA into national digital initiatives like Digital India and partnering with regulatory bodies could ensure that the standard is embedded in content verification processes across sectors.

The government may also consider setting up a committee or task force for evaluating these globally accepted standards, driving alignment within Indian companies to adopt the same, and implementing pilot projects to demonstrate the working and benefits. This is similar to the National Institute of Standards and Technology (NIST), a US government body that set up a task force called Testing Risks of AI for National Security Taskforce for measuring and evaluating AI models used in national security, radiological and nuclear security, cybersecurity, and critical infrastructure to identify the risks.[52] The goal is to enable safe and secure AI innovation, keeping in mind economic growth and public safety.

50. Section 2(t), The Digital Personal Data Protection Act of 2023 (Act No. 22 of 2023)

51. supra note 21

NIST published a report in 2024 examining the potential of standards and techniques for authenticating content and tracking its provenance, labelling synthetic content through watermarking, detecting synthetic content, and preventing generative AI from producing non-consensual intimate imagery of real individuals.[53] The report intends to communicate to various sectors that synthetic content provenance, detection, labelling, and authentication techniques and processes are important to support trust between content producers, distributors like media platforms, and the public. The report makes mention of C2PA as an important part of the content authentication ecosystem.

The government could also consider collaborating with C2PA, just as the French government had done. The French Embassy in Washington, D.C., in collaboration with C2PA, conducted an international briefing in October 2024 on content authenticity and content credentials, with participation from representatives from G20 nations and other aligned countries to discuss the challenges and opportunities presented by AI and the importance of authenticity and transparency in digital content to mitigate the associated risks by building scientific consensus, developing open technical solutions, and defining common international standards.[54]

11.3 Collaboration with Industry Bodies

Collaboration with industry bodies can play a crucial role in driving C2PA adoption. Organizations such as the Internet and Mobile Association of India, Media and Entertainment Skills Council, Confederation of Indian Industry, Federation of Indian Chambers of Commerce and Industry and National Association of Software and Service Companies can advocate for C2PA standards within their networks and facilitate public-private partnerships. These bodies can facilitate knowledge-sharing through workshops, seminars, innovation hubs, and pilot projects, showcasing the benefits of provenance technology in combating misinformation and protecting digital rights. Industry bodies can also work with media companies, digital platforms, and tech startups to integrate C2PA into existing workflows, ensuring smooth implementation. Furthermore, their engagement with policymakers can help align C2PA standards with national regulations. Being industry leaders operating in distinct sectors, they can also serve as guides, providing training programs and certification initiatives equipping professionals with the skills needed to implement and maintain C2PA technologies, assuring that C2PA solutions are practical, scalable, and cost-effective by demonstrating the results and benefits.

52. Alexandra Kelly, NIST sets up new task force on AI and national security, Defence One, November 2024, https://www.defenseone.com/policy/2024/11/nist-sets-new-task-force-ai-and-national-security/401266/#:~:text=Dubbed%20the%20Testing%20Risks%20of,Department%20of%20Homeland%20Security%20and

53. NIST, Reducing Risks Posed by Synthetic Content - An Overview of Technical Approaches to Digital Content Transparency, April 2024, https://www.nist.gov/publications/reducing-risks-posed-synthetic-content-overview-technical-approaches-digital-content

54. C2PA Communications, The C2PA and Embassy of France Collaborate to Advance Authenticity and Transparency in Digital Content, October 2024, https://c2pa.org/post/embasssyoffrance_pr/

A popular example of this on a global level is the European Broadcasting Union (EBU), an alliance of public service media organisations in countries operating within the European Broadcasting Area or which are members of the Council of Europe. EBU had released a position statement calling on the media technology industry to support content provenance and authenticity standards such as C2PA to help audiences trace the origin of content.[55] In this statement, the EBU specifies certain steps including developing comprehensive policies and framework for a unified approach to content authenticity, requiring technology companies, content creators, publishers, content distributors, regulatory bodies, and international organizations to collaborate and proactively work to develop, implement and test open standards such as C2PA standards, and educating the public about the importance of content provenance, equipping them with the tools to critically assess credible sources.

11.4 Alignment with Relevant Laws

For C2PA to be effectively adopted in India, it is pertinent that its working is aligned with applicable IP and data privacy laws. The provenance chain could contradict an individual or entity's IP claim or right. To avoid this, it is essential that C2PA metadata not be used as the basis to establish ownership but simply be relied on to understand the origin and history of actions and changes made to content. Additionally, to ensure compliance with the DPDPA, C2PA specifications must detail how metadata is collected and stored at each stage of creation, publishing, and editing content.

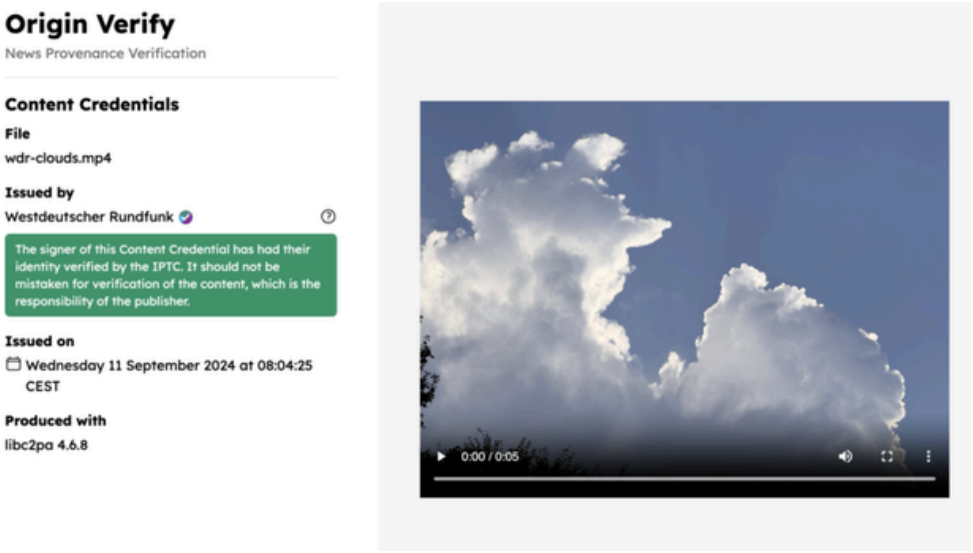


Image No.7- Screenshot of the IPTC Origin Verifier tool showing the content sample from German broadcaster WDR.

55. EBU, Content Provenance and Authenticity TC Statement, August 2024, https://tech.ebu.ch/publications/tc-statement-15-aug-2024-on-content-provenance-and-authenticity

56. Kantar India supported by Google, Indian Languages - Understanding India's Digital News Consumer, 2023, https://services.google.com/fh/files/misc/understanding-indias-digital-news-consumer-2023.pdf

Conclusion

As the digital landscape continues to evolve in India, the proliferation of misinformation and manipulated media poses substantial challenges, especially to research, journalism, social media, and politics. The adoption of C2PA offers a powerful solution and represents a significant step towards enhancing digital content trustworthiness. By implementing C2PA, businesses, influencers, and even the general public in India can benefit from a more secure and trustworthy digital ecosystem. 52% of Indian language internet users read the news online, with 93% of those using YouTube and 88% relying on social media.[56] The time is ripe for both the private and public sectors to come together and establish a roadmap for C2PA adoption, ensuring that India remains at the forefront of digital innovation and integrity. By empowering users with tools for assessing authenticity, restoring trust in media outlets, supporting journalistic integrity, and facilitating cross-platform collaboration, C2PA stands as a pivotal force against disinformation.

However, given the numerous barriers to the effective adoption of C2PA in India including infrastructure limitations, lack of awareness, and legislative and regulatory hurdles, it is imperative to draw support from government entities, private bodies, and other stakeholders, ideally in collaboration to create frameworks that encourage and incentivize adherence to the C2PA standards while addressing privacy concerns associated with metadata usage. Partnerships between technology companies, educational institutions, and media organisations can foster innovation in tools to facilitate easy integration of C2PA into existing workflows.

Provided the initial hurdles are overcome through concerted efforts across multiple fronts, the future of C2PA implementation and use in India appears promising considering the potential benefits for informed public discourse and expression.

YOUR RIGHT TO PLAY

Esports Players Welfare Association, (EPWA) is a New Delhi Based Section 8 Company registered in New Delhi. EPWA is a membership-based players' collective organization with a board of advisors and volunteers assisting us in solving problems faced by skill-based online gamers in India. EPWA currently has around 18,000 members across India. (www.epwa.in). EPWA, conducts research through its research arm EWA Centre.