# Coalition for Content Provenance and Authenticity

## C2PA User Experience Guidance for Implementers

1.0, 2021-12-20: Release

# Table of Contents

# Chapter 1. Introduction

The C2PA intends to provide clear guidance for implementers of provenance-enabled user experiences (UX). Developing these recommendations is an ongoing process that involves diverse stakeholders, with the results balancing uniformity and familiarity with utility and flexibility for users across contexts, platforms, and devices. Our intent is to present a comprehensive range of conventions for the user experience and evolve them based on feedback.

# Chapter 2. Principles

The UX recommendations aim to define best practices for presenting C2PA provenance to consumers. The recommendations strive to describe standard, readily recognizable experiences that:

- provide asset creators a means to capture information and history about the content they are creating, and
- provide asset consumers information and history about the content they are experiencing, thereby empowering them to understand where it came from and decide how much to trust it.

User interfaces designed for the consumption of C2PA provenance must be informed by the context of the asset. C2PA have studied 4 primary user groups and a collection of contexts in which C2PA assets are encountered. These user groups have been defined in the C2PA Guiding Principles as Consumers, Creators, Publishers and Verifiers (or Investigators). To serve the needs of each of these groups across common contexts, exemplary user interfaces are presented for many common cases. These are recommendations, not mandates, and we expect best practices to evolve.

## 2.1. Designing for trust

A unique aspect of this approach is that rather than attempt to determine the veracity of an asset, it enables users to make their own judgement by presenting the most salient and/or comprehensive provenance information. As such it is critical that users develop trust in the system itself, over the individual data presented. Exposing the C2PA Trust Model and Trust Signals in a way that balances transparency and intuitiveness is the critical design goal addressed here. There is no design pattern that can guarantee to engender trustworthiness across multiple contexts, and while C2PA anticipates a degree of contextual customization (see applications and examples), C2PA recommends all implementations adhere to the following general principles.

## 2.2. Quality

Implementations should be created using industry standard, robust user interface technologies.

## 2.3. Accessibility

Implementations should adhere to accepted, current accessibility standards to ensure no users are excluded. For an example of such criteria, see the Web Content Accessibility Guidelines (WCAG).

## 2.4. Consistency

Wherever suitable, UX patterns should match those outlined here. In the case that this would break contextual paradigms of the platform, lean on precedent whether in the OS or app design. Users should not have to learn new paradigms or terminology in different contexts in order to access the information.

## 2.5. Summary vs comprehensive

In many cases, a subset of the available information will be the most useful to a user in a given context. A link through to the full information should always be made available, however.

## 2.6. Linked

Some data will assert an individual or organization, wherever possible, a links out should be made available, to allow the user to make a judgement on those actors' trustworthiness.

# Chapter 3. User experience overview

## 3.1. Levels of Information Disclosure

Because the complete set of C2PA data for a given asset can be overwhelming to a user, C2PA describes 4 levels of progressive disclosure which guide the designs:

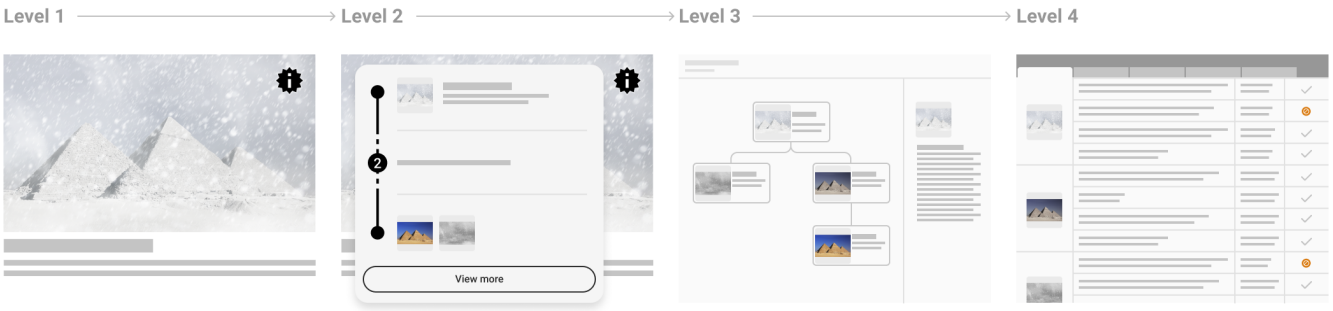


*Figure 1. Disclosure levels*

**Level 1**

An indication that C2PA data is present and its cryptographic validation status.

**Level 2**

A summary of C2PA data available for a given asset. Should provide enough information for the particular content, user, and context to allow the consumer to understand to a sufficient degree how the asset came to its current state.

**Level 3**

A detailed display of all relevant provenance data. Note that the relevance of certain items over others is contextual and determined by the UX implementer.

**Level 4**

For sophisticated, forensic investigatory usage, a standalone tool capable of revealing all the granular detail of signatures and trust signals is recommended. In addition to these standard levels, there will be common tools available for those interested in a full forensic view of the provenance data. This would reveal all available C2PA data across all manifests for an asset, including signature details.

# Chapter 4. L1 – indicator of C2PA data

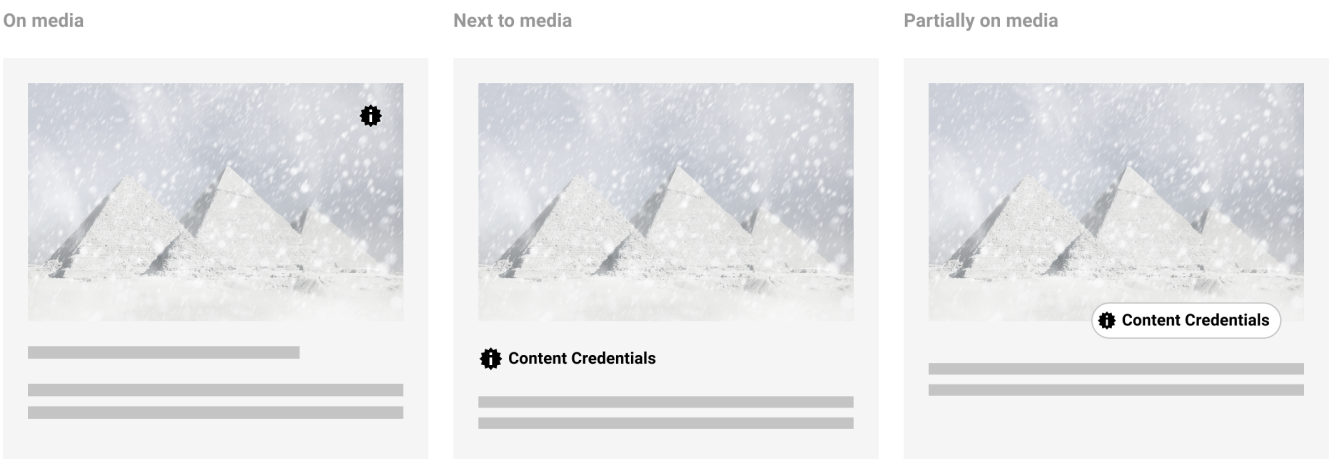


*Figure 2. The L1 indicator*

## 4.1. Appearance

Following the consistency principle, it is important in developing trust that users can learn to easily recognize the presence of the system and that their expectations are met regardless of context. As such, the L1 indicator should be consistent in its appearance across all contexts and devices to the degree that it clearly represents the presence of C2PA data. L1 can be applied using only the icon, the title, or both. If using the icon alone, ensure its appearance meets accessibility criteria so that consumers can easily identify its presence on or near the C2PA-enabled content. We recommend using the placeholder “information seal” icon and working title “Content Credentials” for recognition and learned understanding of C2PA-enabled content. We may make updates to the icon and product name in upcoming versions of this document as we gather findings from on-going user research.

## 4.2. Placement and interaction

For flexibility across implementations, there are several recommended placements for L1 indicators when C2PA-enabled content is present: on top of the content or somewhere close enough that its relationship to the content is clear. If L1 is positioned on top of the content, a hover state may be applied so as not to permanently obstruct the content below. Applications may differ depending on device, such as revealing L1 via long-press on mobile. Partially overlapping the L1 indicator over content is the most robust option to avoid potential misuse in the scenario that it has been purposefully added to content in a way meant to deceive. A new user experience guidance is recommended for initial implementation rollout to make clear how to identify L1 indicators.

Behaviour of L1 indicators should reveal L2 progressive disclosure, either via a hover or click interaction. Within L2 user interfaces, L1 can continue to be used to indicate the presence of C2PA-enabled ingredients.

# 4.3. Validation States

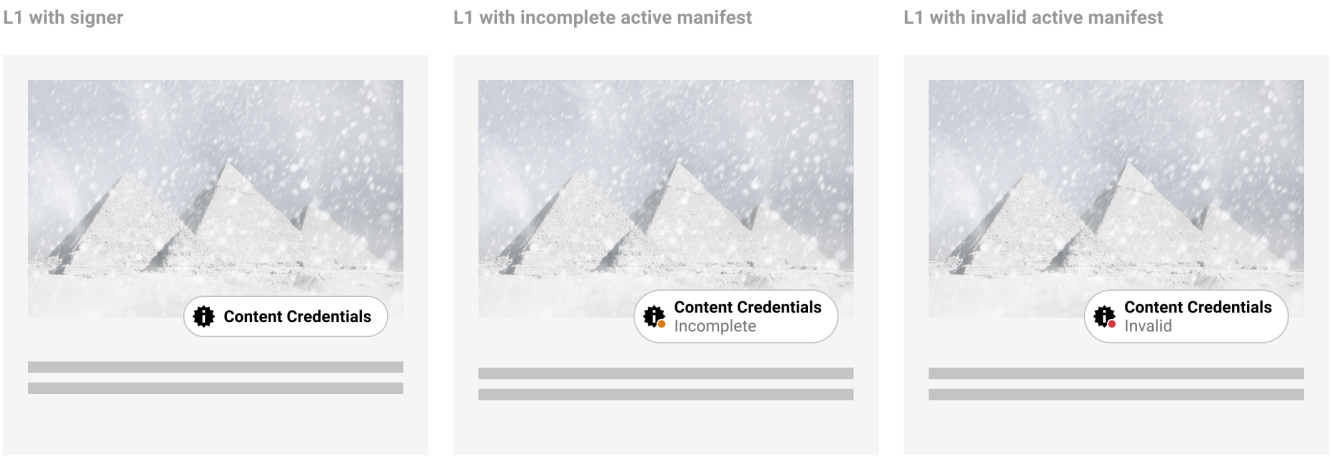


*Figure 3. L1 validation states*

In the event that the active manifest is incomplete or invalid, a stateful indicator of data validation can be displayed. There are several scenarios when displaying a data validation state may be necessary. See Chapter 14. Validation in the C2PA Technical Specifications [insert link] for further information.

# Chapter 5. L2 – progressive disclosures

## 5.1. Minimum viable provenance

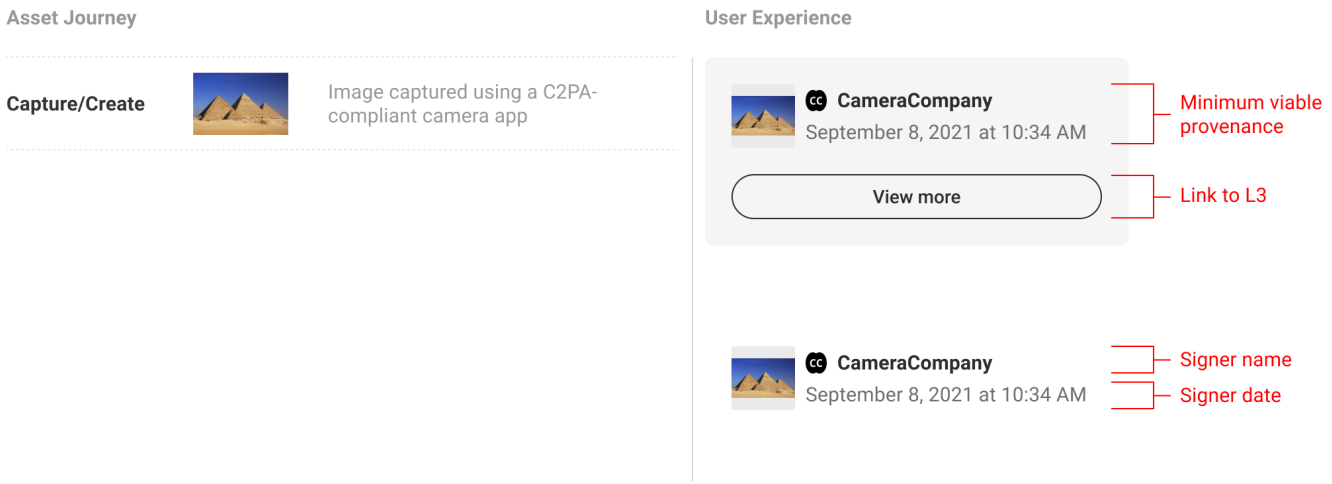


*Figure 4. Minimum viable provenance display*

If L1 indicates the presence of C2PA data, L2 is where consumers can begin to view and interact with the data. The minimum L2 user experience is defined as the display of nothing more than the base required C2PA manifest data: the signing entity, the claim generator and date. The signer is a top trust signal that allows the consumers to make their judgement trusting that the information available has been 'backed' by a legitimate entity. C2PA anticipates that additional varying assertion data will be included by implementers, and recommend including the manifest thumbnail, signer logo, and a link to L3 where consumers can find more assertion data if available.

L2 styles, fonts, etc. can be customized to fit the given context. Iconography and terminology used to describe assertions should be consistent wherever possible. C2PA anticipates the need for L2 generally to be real-estate efficient as it appears within the implementer's context, so C2PA suggests streamlining the data displayed to provide enough information for the particular content, user, and context to allow the consumer to understand to a sufficient degree how the asset came to its current state.

## 5.2. Manifest Summaries

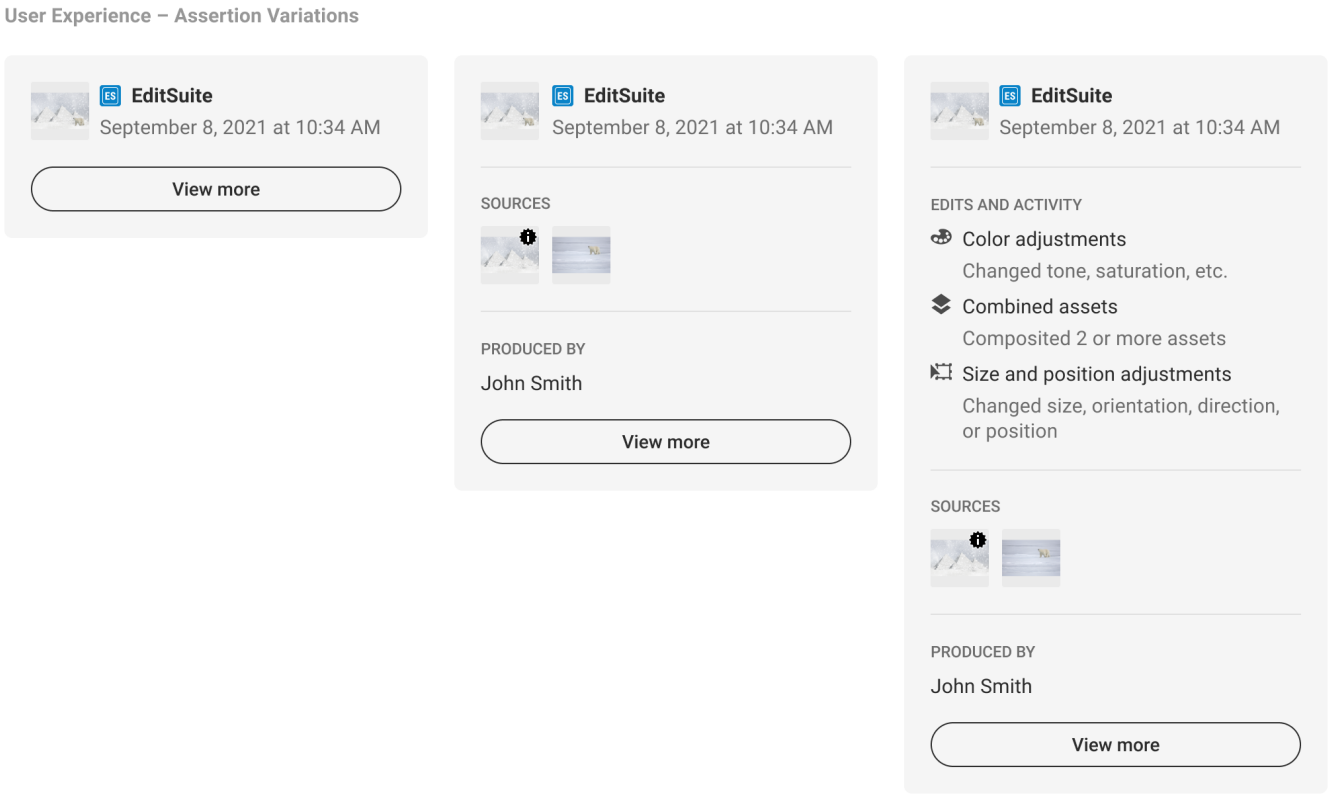


*Figure 5. Single manifest displays*

A discrete manifest display only represents a single manifest. It could be the active manifest, as this is the most recent version tied to the C2PA-enabled content, or another manifest determined by the implementer. The determination for displaying a discrete manifest should be if there is substantive assertion data in a given manifest the implementer believes is most relevant to its audience. A shortcoming of discrete displays it that the highlighted manifest may not represent the complete history of the C2PA-enabled content, and may require consumers to navigate away from the implementer's context to L3 to learn more.

## 5.3. Summary displays

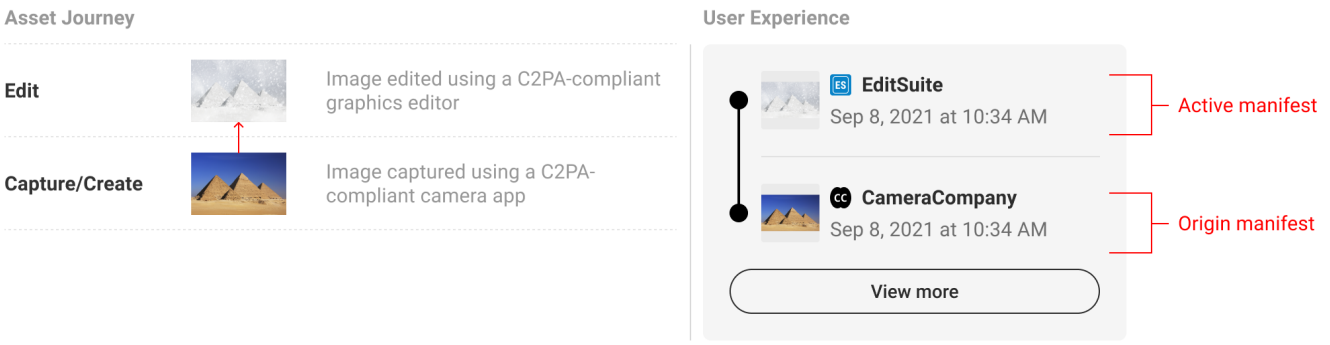


*Figure 6. Summary display, example 1*

A provenance summary display represents the collection of manifests related to the C2PA-enabled content. Manifests

should be presented in reverse chronological order, starting with the active manifest at the top and the origin ingredients below. Origin ingredients represent the beginning of their respective history branches.

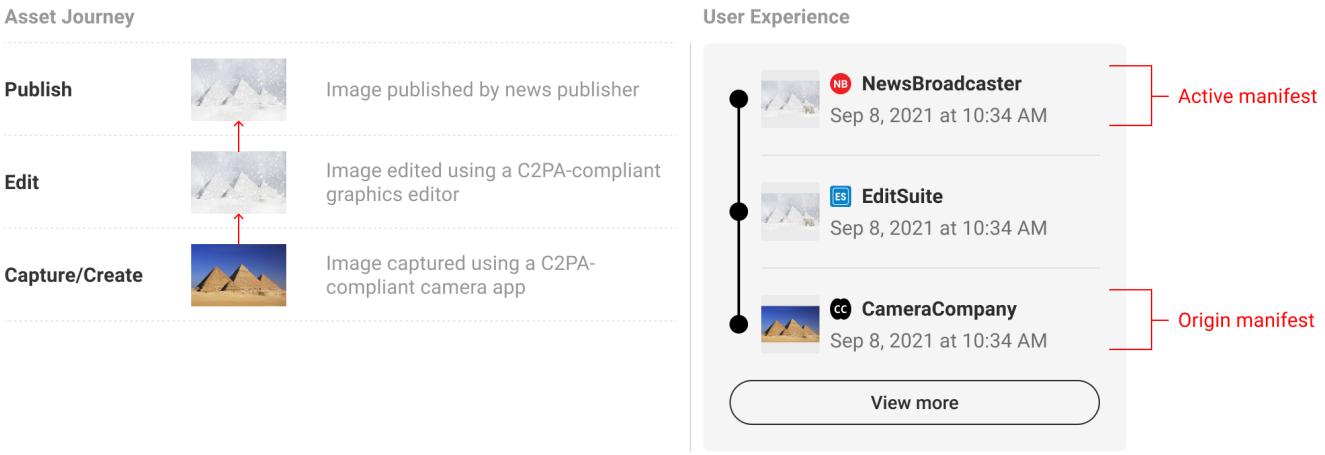


*Figure 7. Summary display, example 2*

Summary displays should show at minimum the origin ingredients and active manifests, or if screen real estate allows, with at least one manifest in between.

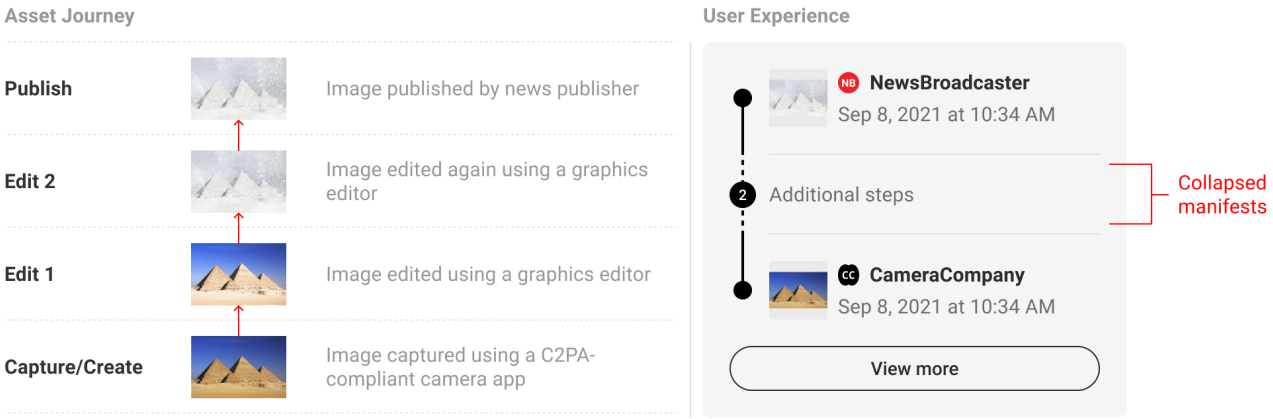


*Figure 8. Summary display, example 3*

In order to provide users with a succinct summary and to allow for limited screen real estate, the manifests in between origin and active can be collapsed and represented as a numerical count. C2PA recommends a baseline rule for collapsing manifests if the total number exceeds four or more. However, this threshold can be altered according to context. In keeping with the core recommendations, a link to the full set of data in L3 should always follow the summary list of manifests.

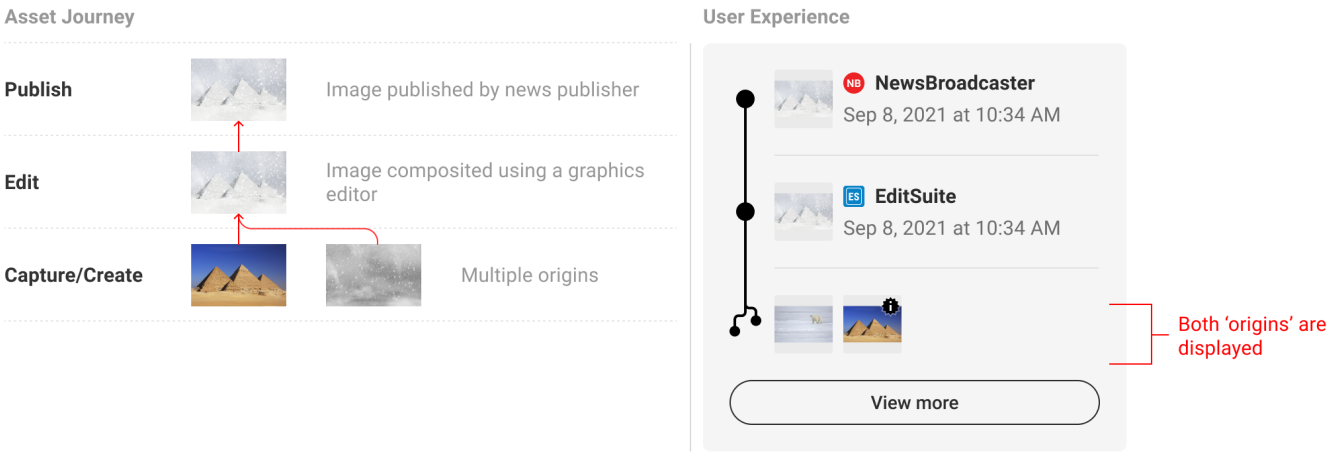


*Figure 9. Summary display, two origins*

When multiple origins are present, either as multiple ingredients in a single manifest or across multiple manifests, they can be summarized in the origin section of the UI. The L1 indicator can be used as a badge on ingredient thumbnails to distinguish C2PA-enabled assets.

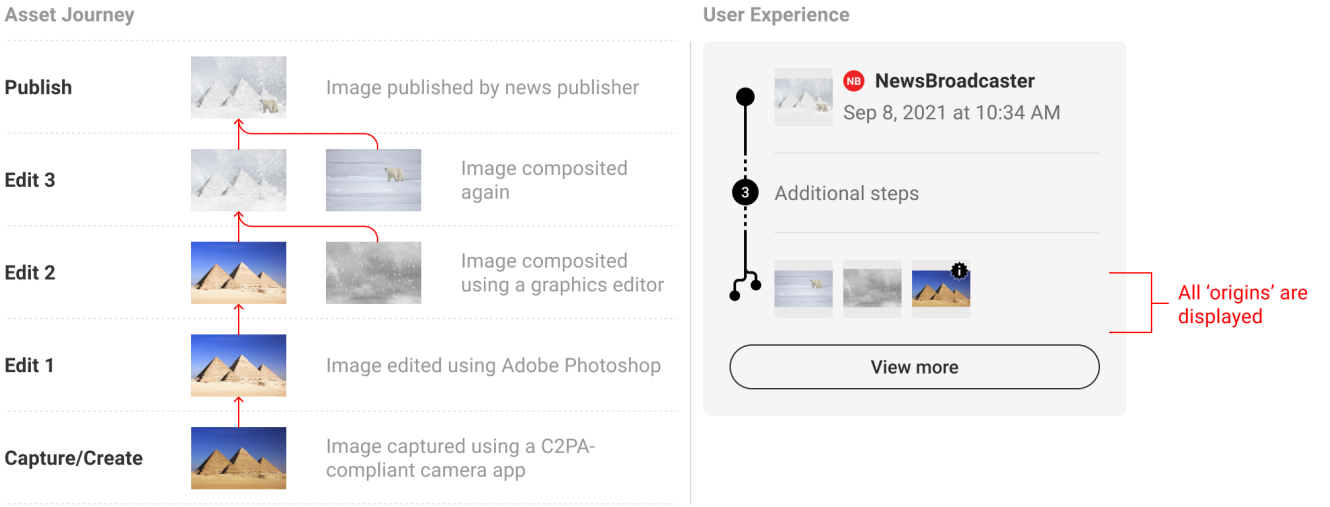


*Figure 10. Summary display, multiple origins*

L2 UI is flexible enough to allow for various combinations of manifest counts and origin assets.

## 5.4. Validation states

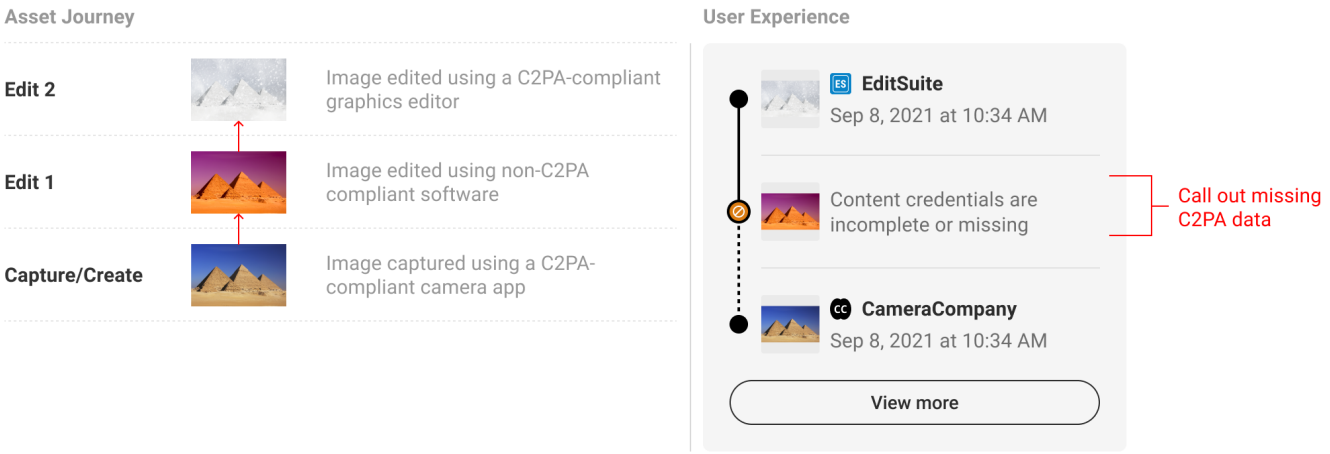


*Figure 11. Incomplete data, example 1*

There will be instances when C2PA-enabled content is incomplete data. Most commonly, this will happen if the content is edited without capturing C2PA data. In this event, the L2 and L3 UI should reflect when data is incomplete, as well as the manifest data that came before or after. A dotted line can be drawn between manifests to suggest the connection is not the same as between valid, intact manifests. Incomplete data should not automatically signal that one should discount the content as untrustworthy. For this reason, C2PA discourages the use of an indicator designed to trigger alarm, which should be reserved for more apparent tamper-evident use cases, in favour of a more descriptive and neutral indicator.

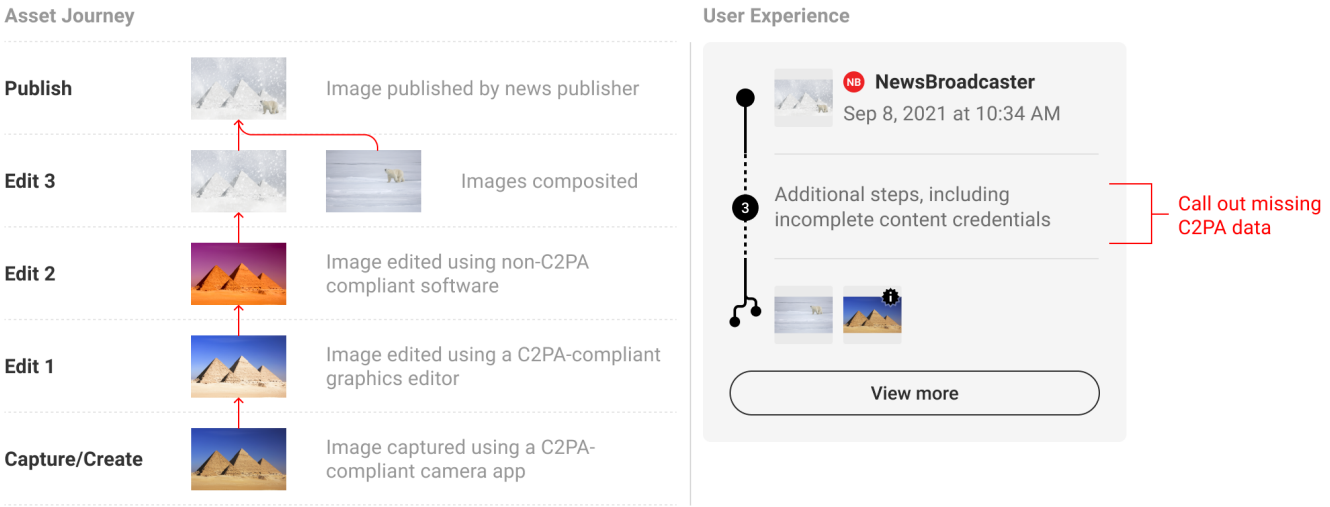


*Figure 12. Incomplete data, example 2*

Following the established pattern of collapsing additional manifest, incomplete data can be called out via the text string (Figure 13) to bring awareness to the questionable validity of ingredients.

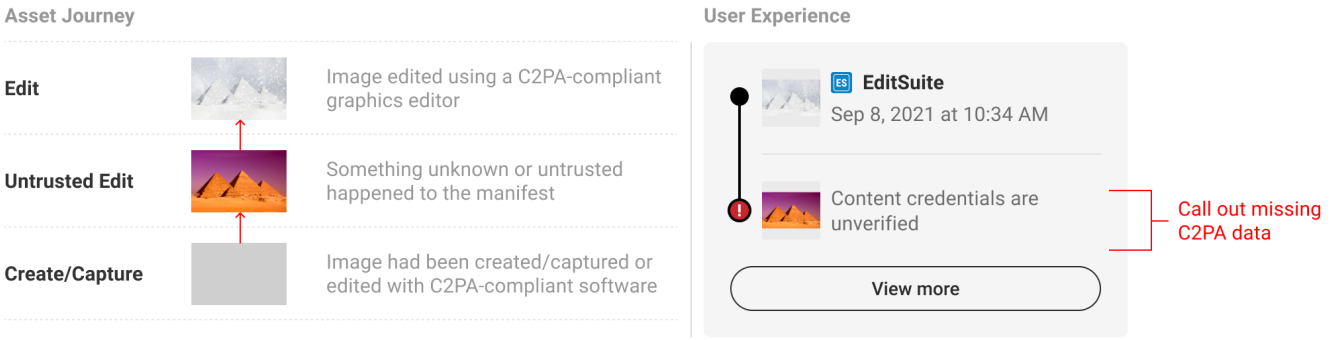


*Figure 13. Invalid display*

There may be instances when C2PA-enabled content has been maliciously edited to tamper with C2PA data, or is signed by an untrustworthy entity. In this case, no additional prior data can be displayed.

# Chapter 6. Applications and Use cases

As above, L2 assumes some level of contextual customization will be beneficial to make C2PA data helpful to users. Rather than recommend customizations based on a fixed set of applications, instead C2PA has categorized the ways that assets are used to communicate aspects of reality to users, and provide a recommended customization based on that. The following examples represent a range of potentially common applications:

## 6.1. Arts and entertainment

Depicted is a discrete manifest showing an identity assertion, indicating the uploader is the same as the content producer.

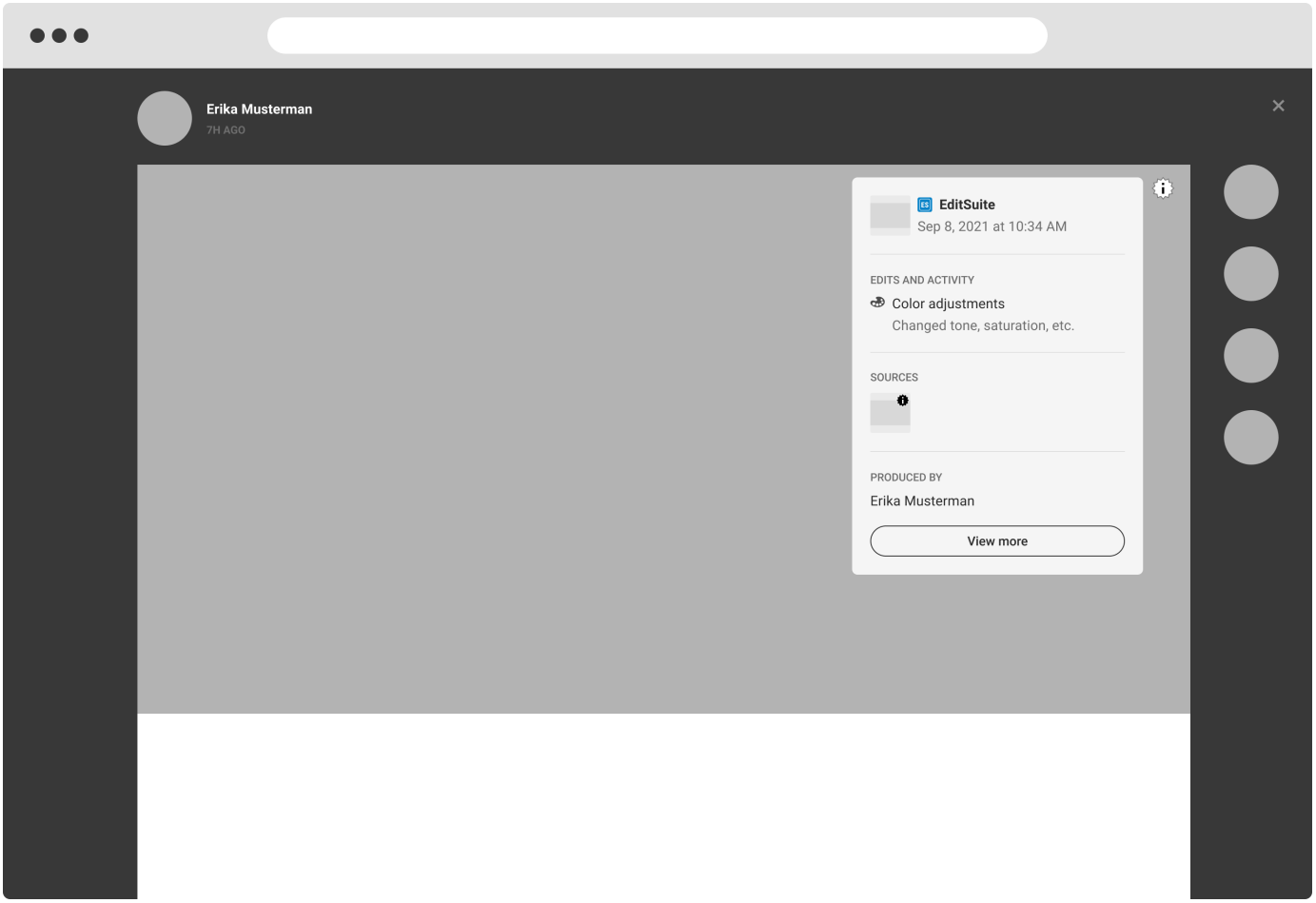


*Figure 14. Entertainment example*

## 6.2. News

An example of photojournalism, wherein steps between the origin and published manifests are displayed.

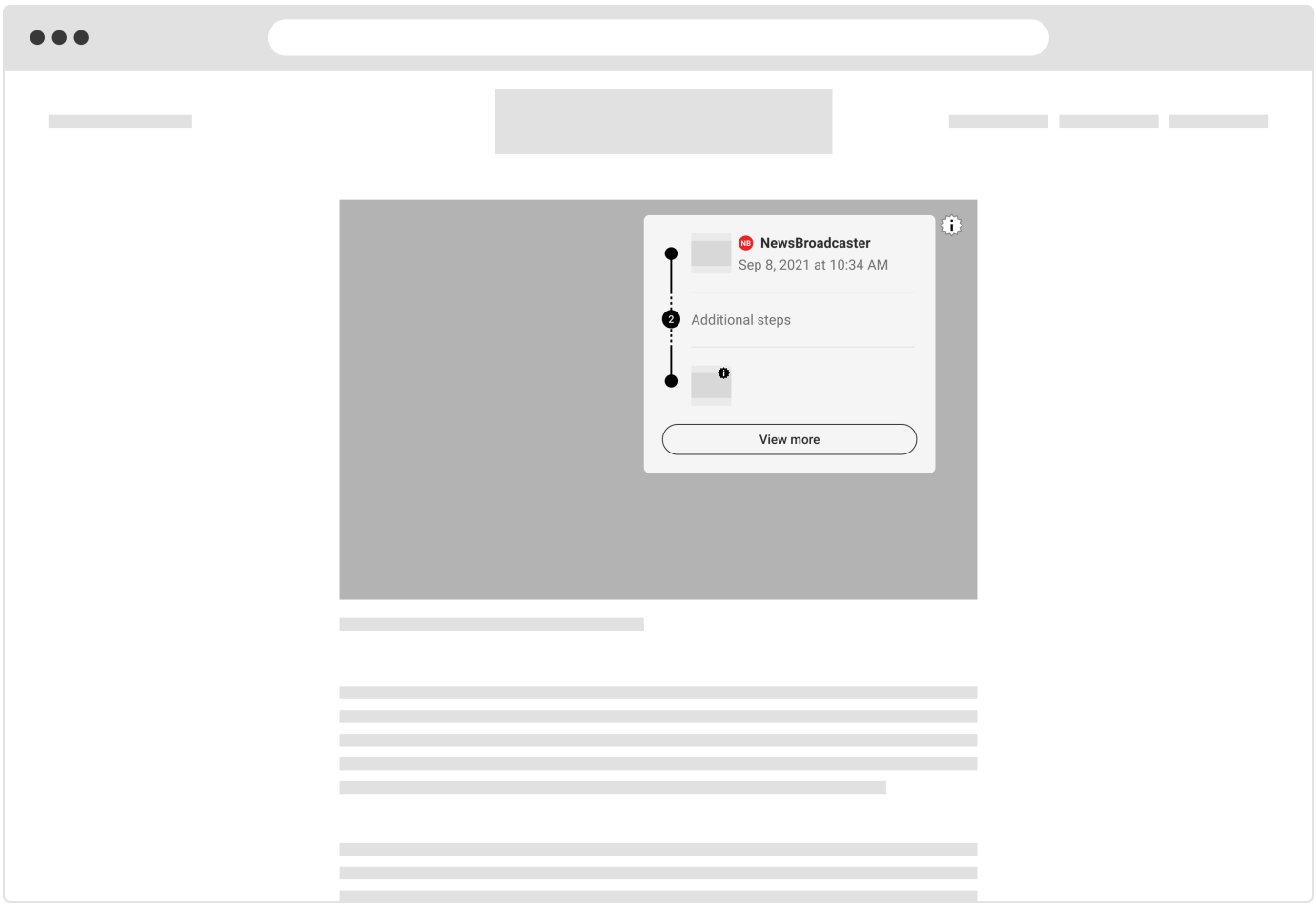


*Figure 15. News example*

## 6.3. E-commerce and retail

Depicted is a more complex summary, indicating the shared content on the retail platform is an edited composite of two images. Buyer beware!

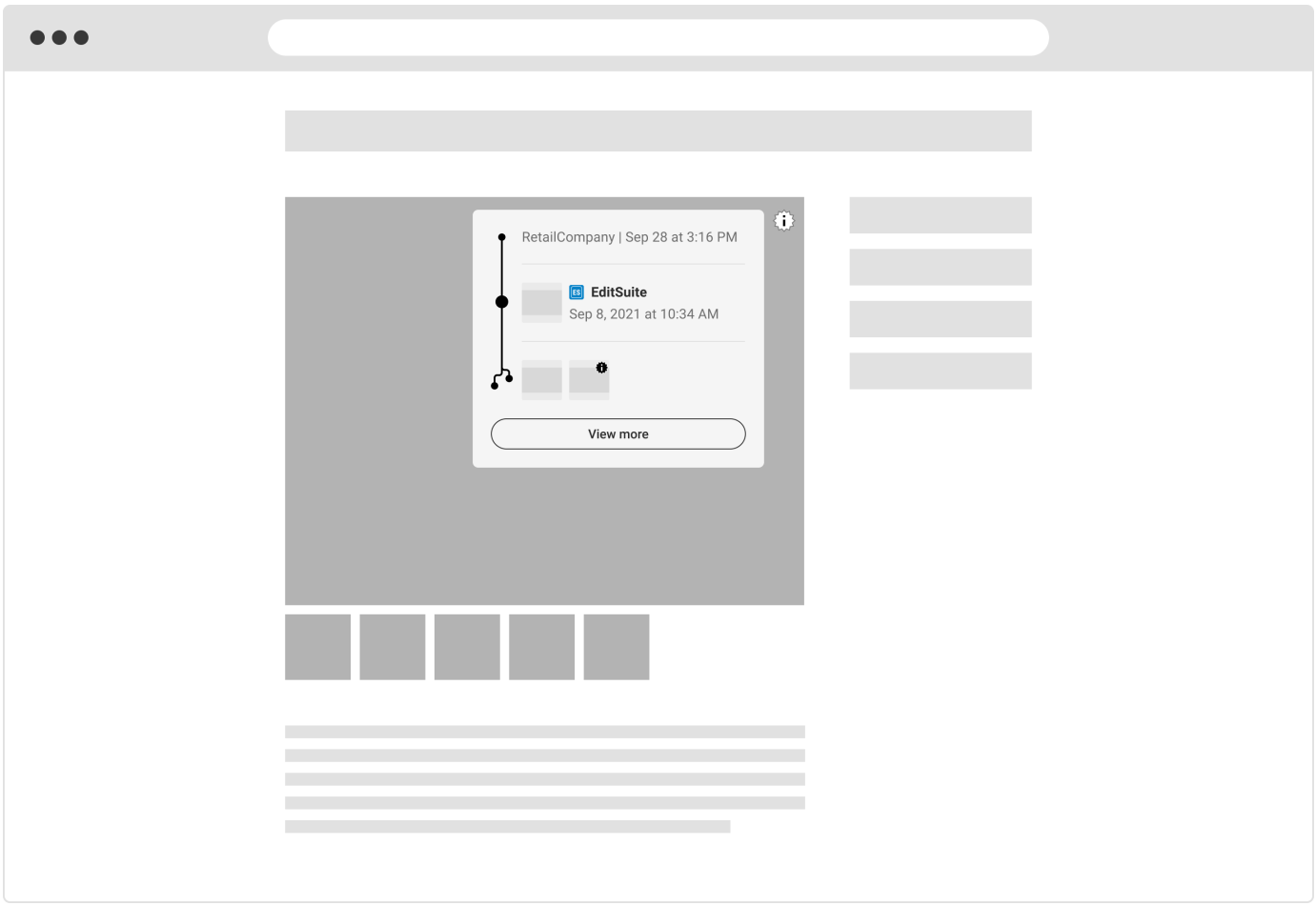


*Figure 16. E-commerce example*

## 6.4. Travel

A travel company publishing a photo captured by a C2PA-enabled camera app.

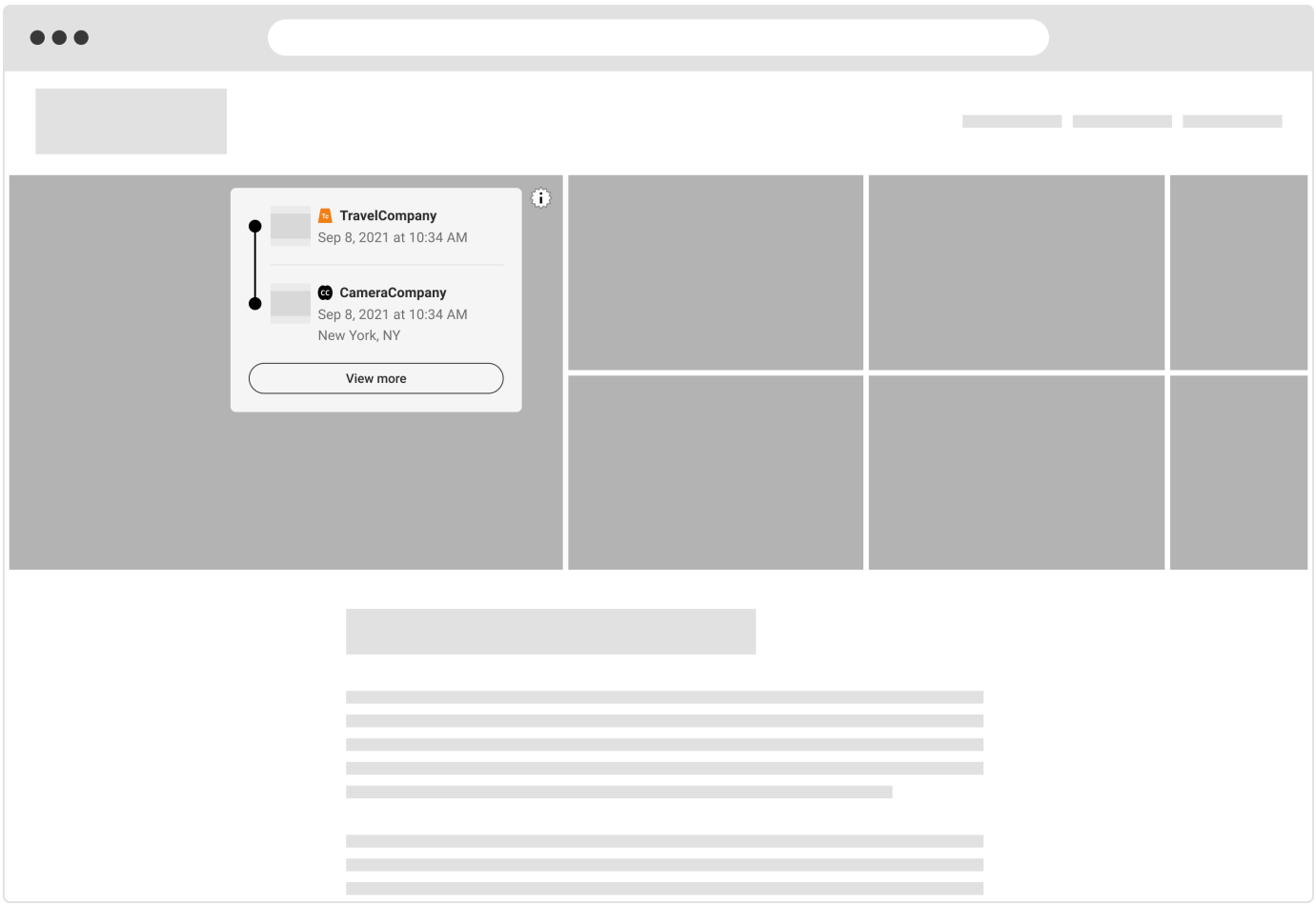


*Figure 17. Travel example*

# Chapter 7. Creator Experience

## 7.1. Opting in, user privacy and data collection

As per the C2PA Guiding Principles, C2PA implementations should provide a mechanism for creators of a given content to assert, in a verifiable manner, any information they wish to disclose about the creation of that content and any actions taken since the asset's creation. As such, the creator experience requires the following:

A clear acknowledgement of user consent before a C2PA implementation can begin accumulating data; Disclosure or preview of the nature of information that is being recorded; User control over recorded information, with particular sensitivity to the creator's identity and process. C2PA recommends an opt-in flow that concisely represents these requirements and can be opted-out of just as easily at any time. Once opted-in, users should be able to distinguish between non-removable information as defined by the C2PA specifications and information that can be adjusted according to the user's preferences.

## 7.2. User settings and claim preview

(Wireframe of settings and preview UI)

Users should be able to control the information in their assertions as much as is allowed by C2PA specifications. The Harms Modelling document covers the reasoning behind why user control is imperative. To provide coverage against harms and misuse, C2PA suggests the following types of assertions be manageable by the user:

- Identity information
- Actions
- Creative Work
- Fields pertaining to copyright, descriptions, and usage rights
- Exif information and related metadata

To be accommodating to the user's preferences, C2PA recommends presenting a UI wherein these assertion categories can be toggled on or off on a per document basis. To assist the user in understanding the tradeoffs they are making, C2PA also suggests displaying a claim preview that concisely and accurately depicts what information will be added into the manifest.

## 7.3. Identity

The identity of the creator, or lack thereof, is an important assertion for the completion of a content's provenance as it helps consumers understand the person(s) responsible for what happened. It is important to restate that C2PA specifications do not require the identities of persons or organizations making any assertion or claim about an asset to be documented. However, the challenge of validating identity when provided is beyond the scope of the C2PA specification at present. As such, C2PA recommends several tactics to help consumers understand the role of identity

in C2PA provenance data.

The first is to make clear when the producer's identity is self-assigned. The second is to offer creators the ability to add social media or other verifiable accounts. These identity flows may lie outside of C2PA creator implementations, but when included, have the added benefit of providing social proof for creators as well as links out to their presence elsewhere on the internet.

When the user decides to opt out of including their identity information, C2PA recommends promptly updating the claim preview to reflect this change to give the user immediate assurance their privacy is being protected.

## 7.4. Actions

Similar to the treatment of identity, some users may want to reserve the right to not disclose the actions they've taken on a given content. While some use cases, like photojournalism, should always show transparently what actions took place, this is less important for more creative and artistic applications. In some cases, users may want to protect their particular process of creation and should therefore be allowed to opt out of including actions in their claims.

Granularity of actions is worth considering in creator implementations. In some cases, grouping actions into high level categories may be more understandable for consumers, versus presenting a list of detailed, creation-specific actions that may be unique to the implementation. C2PA recommends striking a balance between clarity and information overload based on the intended audience of the implementing platform.

## 7.5. Ingredients and their validation state

(Wireframe of preview UI with ingredient validation states)

Ingredient assertions represent a form of non-removable information because they are the key to the establishment of the provenance of an asset and may themselves contain provenance. As such, ingredients are a requirement to be displayed in the claim and its creator-side preview.

Validation of an ingredient's manifest is equally important to convey to users prior to producing a new claim. Within the claim preview UI, C2PA recommends displaying a list of ingredient thumbnails and their validation states to ensure the user working with those ingredients is aware of additional provenance data. This is particularly important for cases when ingredients are unable to validate or contain an invalid manifest. A clear example might be a news editor who receives a piece of user-generated content that purports to depict a controversial scene - alerting the editor to the validation state of that image will give them stronger assurances of whether that content is trustworthy.

## 7.6. Error handling

Work in progress.

## 7.7. Exporting

The C2PA Implementation Guidance recommends that a manifest be created for an asset when a significant event in the lifecycle of the asset takes place, such as its initial creation or an "export" operation from an editing tool. This is in part due to the underlying technical process of digitally signing the claim, but also aligns with natural creation workflows. When a user is ready to export their work, they should be able to decide whether or not to attach the accumulated claim data to their content. Not every piece of exported content is in need of provenance data, so C2PA recommends enabling the option of attachment on a per document basis. It will also help serve as a reminder to users that they have opted into the C2PA implementation, which will allow them to protect their privacy as needed.

# Chapter 8. Open issues

## 8.1. Video

As a time-based media, video provenance represents a significant challenge to distill into simple consumer UI. Topics the C2PA are actively exploring relate to the visual representation of ingredients, the volume of potential edits, and assertions tied to temporal segments. C2PA aima to provide more detailed recommendations for video content by the v1.0 spec.

## 8.2. User research

Correctly identifying and displaying trust signals are a paramount concern for our overall user experience. C2PA strives to understand the value consumers will apply to content attribution through ongoing user research studies and usability testing.

# Chapter 9. Public Review, Feedback and Evolution

The team authoring the UX recommendations is cognizant of its limitations and potential biases, recognizing that feedback, review, user testing and ongoing evolution is a requirement for success. This guidance is therefore an evolving document, informed by real world experiences deploying C2PA UX across a wide variety of applications and scenarios.