

Bill Study:

AI Labeling and Provenance

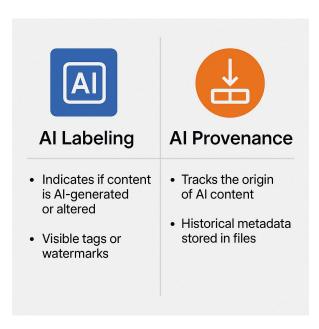
Presented by Navya Annapareddy, Ph.D Candidate, UVA School of Data Science



What is AI Labeling and Provenance?

Provenance - The record of where AI data and models come from, how they were built, and how outputs were generated.

Labeling - The disclosure to users that content was created or modified by AI, often through tags, watermarks, or metadata.





Key Concepts

Watermarks - Visible or invisible markers embedded in AI outputs that signal synthetic origin or modification.

Material Transformation - Occurs when AI alters authentically human-captured content substantially such that the result no longer represents the original capture but instead constitutes AI-generated content.

- ie: replacing, generating, or re-synthesizing core elements



Key Concepts

Portability - The ability for provenance and labeling information to travel with content across different platforms and formats.

Persistent - The requirement that provenance and labels remain intact through transformations like editing, compression, or sharing.

Tamper-evident - A system that shows when provenance or labels have been altered or removed, signaling possible manipulation.



Policy Issues

Provenance and labeling systems are **fragmented**, **proprietary**, and often **non-interoperable**.

Existing consumer protection laws do not provide clear, proactive labeling requirements.



Policy Recommendations

- (1) Focus on **labeling authentic and trusted content** via flexible labeling approaches like authenticity markers and voluntary AI tags.
- (2) Do not require a specific provenance standard.
- (3) Require platforms to reasonably **carry forward provenance data** when content is uploaded or shared.



Additional Considerations

The limits of provenance

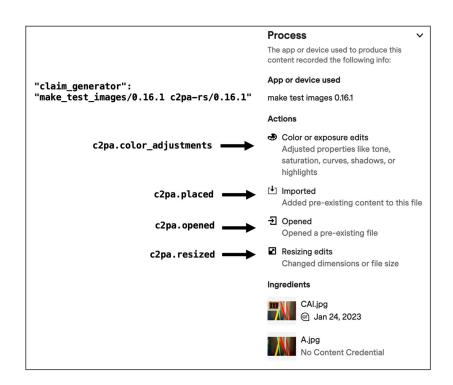
- Portability across platforms
- Persistence through editing and sharing

Meaningful labeling for the public

- Visibility and clarity of tags
- Differentiating tiers of AI-generation

Innovation and competition

- Avoiding one-size-fits-all standards
- Interoperability without lock-in





Thank You