BRIDGE LABS

# Advancements in Digital Rights Management

## From Consent to Technological Solutions

**Practical Solutions for Content Creators in the Age of AI**

**Peng Boris Akebuon**

Co-Founder and CTO

# We can protect creative works in the Age of AI while fostering innovation.

Let’s see how!

# The Legal Issue with Gen AI

"The legal issue with gen AI is that to create the model, we have to copy many many work."

Ian B. Crosby

Can Copyright Law Stop Gen AI?

# Digital Right Management

Digital Right Management (DRM) permits us to manage the legal access to digital content. This involves using tools and technologies that can restrict the access to copyrighted content.

**Limitations of existing DRM solutions:**

- Digital flags, metadata, watermarks, and signatures are great but easy to remove or alter.

- Difficulty in applying solutions across different media types and platforms (text, images, video).

# AI Training Data

Massive amount of data is been scraped from the internet without the consent of content creators and it’s usually used to create products that competes with the creators.

- Difficulty in identifying copyrighted material.
- Lack of transparency and creator consent.
- Potential for infringement and plagiarism.

# 3 Practical Solutions

Use these methods to protect your creative works today.

## 1 Opt-Out mechanisms

Platforms like "Have I Been Trained?" permits content creators to register their works and opt-out of AI training use.

## 2 Data Poisoning

The manipulation or contamination of data used to train machine learning models. E.g Glazing and Nightshading

## 3 Restrict Public Access

Limiting the availability of the creative content to the general public, thereby reducing the likelihood of it being copied or exploited without permission.

[Protect Your Art From AI]

# Split View Protection

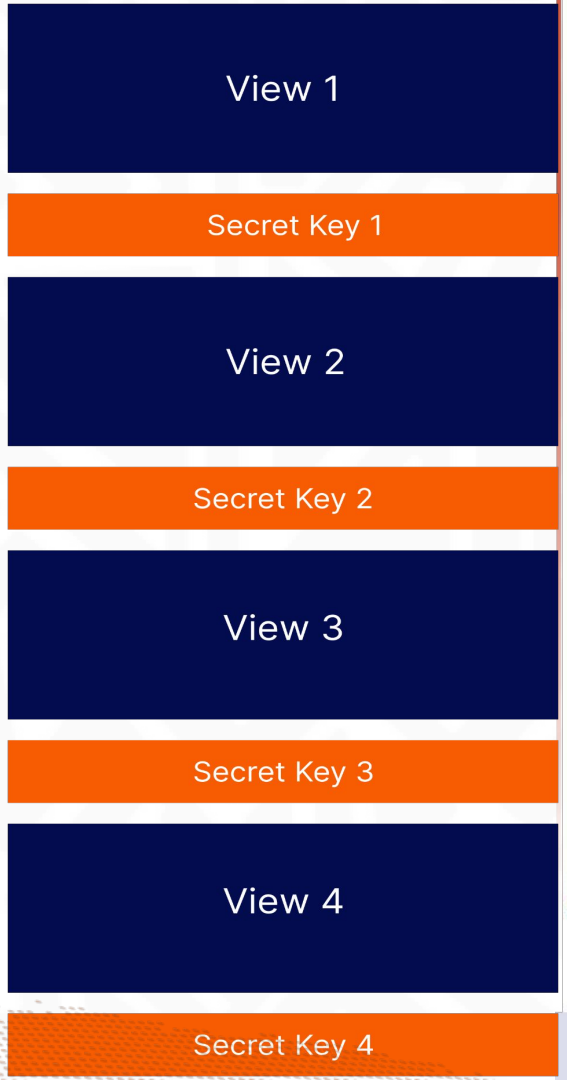
This technique leverages the dynamic nature of online content to ensure that unauthorized data scrapers capture a "**poisoned**" or "**incomplete**" version of the work, rendering it unusable for training AI models.

- When a user accesses your protected content, it's split into multiple views on the server-side.
- Each view is embedded with a **unique, invisible signature** acting as a security measure.

Inspired by **split-view poisoning**

# Split View Protection

- To access the full work or next view, users need the valid signature from the previous view.
- If an unauthorized bot or scraper attempts access, they receive:
  - **Poisoned content:** Unusable for AI training due to missing information.
  - **Restricted access:** The content is completely blocked.



# Split View Protection

**Benefits:**

- **Control Over Usage:** Creators can choose to offer Split-View Protection for their work, granting access only to authorized users.
- **Enforced Consent:** The signature system prevents unauthorized data scraping for AI training without the creator's consent.
- **Transparency:** Users encountering Split-View understand the content is protected and creator consent is required for full access.

# Split View Protection

**Limitations:**

- **Scalability:** Implementing this technology across various platforms and content types needs further exploration.
- **Efficiency:** Ongoing development is necessary to optimize performance.
- **Bypassing Techniques:** Malicious actors might develop methods to appear legitimate.

# Useful Resources

- AI vs Artists - The Biggest Art Heist in History
- 4 Easy Ways To Protect Your Website Content from ChatGPT and AI Models
- ChatGPT and Generative AI Are Hits! Can Copyright Law Stop Them?
- This new data poisoning tool lets artists fight back against generative AI | MIT Technology Review
- About | Have I Been Trained?
- Protect your Art from AI

BRIDGE LABS

# THANK YOU


**Peng Boris Akebuon**

Co-Founder and CTO

peng@bridgelabs.tech