

£10 / €10

iaU!

JOURNAL

Change management for the creative industries

AUTUMN 2025

au-works.com

**HOW TO FIGHT
A PACK OF
PIRATES**

**SURVIVING
THE GEN AI
BUBBLE**

**ON THE TRAIL OF
THE GHOST
INFLUENCERS**

**HUNGRY
FOR YOUR
CONTENT**

OUR IP DEFENSE SPECIAL





We Stop Piracy

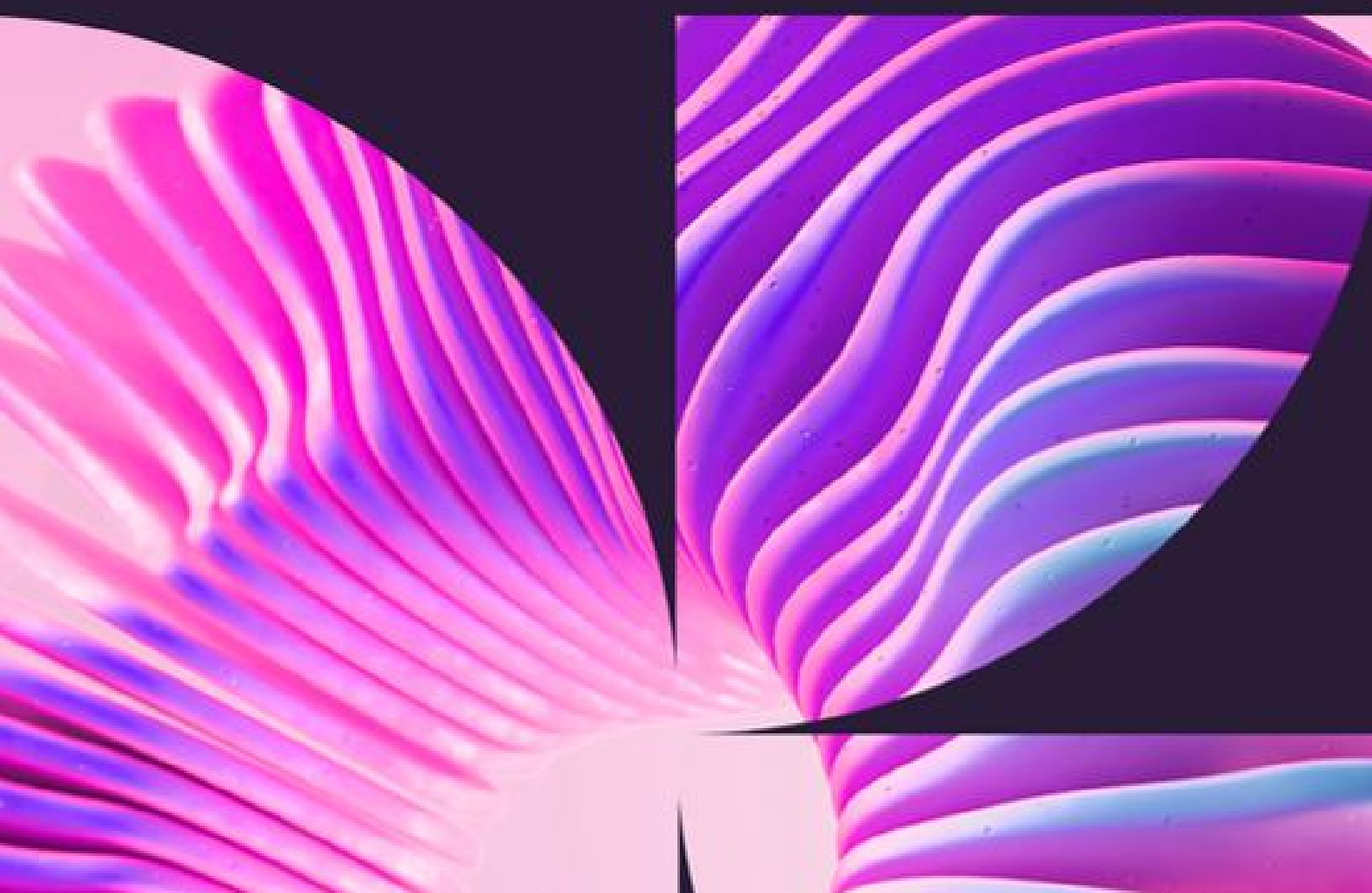
The world's most effective
anti-piracy solutions.

 Monitor

 Identify

 Disrupt

friendmts.com



EDITORIAL DIRECTOR

Neal Romanek
+44 (0) 754 508 7629
nromanek@au-works.com

CONTRIBUTORS

Tommy Flanagan, Graham Lovelace

IMAGES & PHOTOGRAPHY

Estefano Burmistrov, Silvia
Gaudenzi, Pete Linforth,
Creature SH

iAU!

jAU!

69 Rosebank Road
London
W7 2EW UK
au-works.com

For content & storytelling
editorial@au-works.com

For advertising & partnerships
partners@au-works.com

Sign up for our newsletter [here](#)



WILL YOU FIGHT FOR THE FACTS?



Welcome to the second issue of *jAU! Journal*, jAU!'s quarterly deep analysis into the vital issues affecting the media industry, and the wide, wide world.

I like democracy.

Just a BTW.

One of the great things about democracy is you get to complain. About the incompetence—the downright evil—of the other side, and about your own side and how they've let you down.

The reason there's lots of blame to go around in democracy is that actual people choose the government. Real people make real choices. There is accountability. And responsibility. There's a paper trail.

But for it to work, people need a reliable information space. Today we are faced with a complete shattering of what was an imperfect—but kind of stable—system. Now, powered by disinformation, copyright theft, and synthetically produced content, inauthenticity—and irresponsibility—is being manufactured at scale.

Under these circumstances it's hard to sustain self-governance. In a world without responsibility, that enjoyable blame game is replaced by confusion, suspicion, and cynicism.

This issue of jAU! Journal looks at how media businesses are clawing back control over their content and creating islands of authenticity amid the chaos. It's a long journey back to the truth. But we have to make a start, right now.

Neal Romanek
Founder, jAU!

AUTUMN 2025

THE CONTENT & IP SECURITY ISSUE

03 WELCOME

Editorial director Neal Romanek introduces this issue's content protection theme

06 WHAT NOW?

News & briefs on content security from around the industry

10 C2PA ACCELERATOR AT IBC

A look at this year's IBC Accelerator project on real world uses for C2PA

16 IP PREDATORS: THE ANTI-PIRACY ARMS RACE

Our survey on piracy & streaming—and the latest tech defenses

22 C2PA ISN'T A PROTOCOL DROID: IT'S A PLAN FOR FREEDOM

A deep dive into the new tools for tracking content provenance & authenticity

26 **ON THE TRAIL OF THE GHOST INFLUENCERS**

Fake “experts” are being quoted in top publications. The hunt is on.

32 **CONTENT BY NO ONE FOR NO ONE: SURVIVING THE AI BUBBLE**

Can the industry put the brakes on its toxic relationship with AI?

38 **GOVERNMENTS ARE ABANDONING CREATORS TO AI**

In the fight to protect creative businesses, governments are siding with robots

42 **BUILDING AN ARTIST FRIENDLY AI**

Start-up Incantor creates Gen AI tools with creator profitability in mind

46 **NEXT ISSUE**

Our Winter 2025 issue will examine creative sovereignty & controlling your own tools

47 **READ ISSUE ONE!**

*Enjoyed this issue of jAU! Journal?
Go back & read out Summer Issue too!*

WHAT NOW?

News & snapshots

New Danish law for deepfake defense

Denmark has introduced a draft law to combat deepfakes which would give each person copyright control over their appearance and voice. Deepfakes would be illegal to share without the express consent of the person being portrayed.

“We agree and are sending an unequivocal message that everybody has the right to their own body, their own voice and their own facial features, which is apparently not how the current law is protecting people against generative AI,” Danish culture minister, Jakob Engel-Schmidt [told The Guardian](#).

The new law would empower Danes affected by deepfake content to demand its removal or get compensation for unauthorized monetization of their image.

This right to receive a percentage of revenue garnered from deepfake use would extend for 50 years beyond the person’s death. Any platform’s hosting deepfake content could face fines.

The new Danish bill doesn’t explicitly address criminal charges but would set the stage for anyone seeking to pursue damages in court. The draft law will come before the Danish parliament this autumn.

While legislation against AI content has been slow to appear, in May of this year, the US passed the [TAKE IT DOWN](#) (Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks). The law takes aim at nonconsensual publication of “intimate visual depictions of individuals, both authentic and computer-generated” — NCII (non-consensual intimate imagery) or “revenge porn”. The law requires platforms to create a process where victims who have had likenesses posted without consent can notify the platform and expect it to be removed within 48 hours.

Critics of the TAKE IT DOWN Act have expressed concerns about the vagueness of its wording and potential for enabling the fast removal of legitimate content.

Outer Limits pirate service hit with \$15m judgement

The U.S. District Court for the Central District of California has issued a \$15 million judgment against the operator of pirate streaming service Outer Limits IPTV. The service was operated by Zachary DeBarr, who promoted Outer Limits and other illegal services through his YouTube channel.

According to anti-piracy coalition Alliance for Creativity and Entertainment (ACE), Outer Limits provided subscribers with roughly 13,000 film titles, 3000 television series, and 4000 live channels, including international programming and live sports events.

“The court’s favorable ruling against the operator of a commercial-scale digital piracy service marks a significant step forward in our fight against global piracy,” said Karyn Temple, Senior Executive Vice President and Global General Counsel for the [Motion Picture Association](#). “We welcome the \$15 million damages award and the court’s order permanently barring the defendant from further streaming films and TV series without authorization.”

Sports streaming pirate arrested in Argentina

The founder of illegal sports streaming platform Al Ángulo TV, known by the alias “Shishi”, has been arrested in Argentina, following a raid on his home in Paraná, Entre Ríos.

The raid, executed by the Argentine Federal Police and Buenos Aires Provincial Police, under guidance of the Specialized Prosecutor’s Office for Cybercrime (UFEIC) uncovered a tech lab used to operate the piracy network. The Prosecutor’s Office identified “Shishi” as the “founder and sole owner” of the website and app.

Al Ángulo TV streamed illegal broadcasts of football matches and Formula 1 events and used 14 mirror domains to replicate stolen content. The platform also launched an Android app, alangulotv, which gained tens of thousands of viewers. The operation was monetised through advertising. It also is said to have exposed users to malware and data theft. The company’s profits were funneled through cryptocurrency wallets.

The investigation was driven by the [Alliance Against Audiovisual Piracy](#) (ALIANZA), a non-profit organization of members of the Latin American content industry, in partnership with Spanish football federationb LaLiga.



Spanish football fans warned of piracy poison

LaLiga has launched a new [anti-piracy awareness campaign](#) for the new 2025/26 football season. In a press release the league claimed that Spanish football clubs alone lose an estimated €600–700 million annually due to illegal broadcasts and that as much as 50% of online viruses are linked to illegal content.

Under the slogan “You Get Pirated Football, They Get You”, LaLiga aims to highlight that far from being a “victimless crime”, football fans who access pirated content are opening themselves up to risks which could include identity theft, fraud, device hijacking, and privacy violation.

Spain is one of Europe’s top countries for watching pirated content, especially among young audiences, according to the European Union Intellectual Property Office (EUIPO).

YouTube is secretly reversioning user content

YouTube has been altering user video Shorts without permission. The new versions of the content show signs of sharpening and touching up of facial features.

Youtuber Rhett Shull went into detail on his own experience of the changes, with a deeper investigation, [in this video](#) which got half a million views in its first week.

While the reversioned videos have an aesthetic that evokes Gen AI video, YouTube in a post on X said it is not using Gen AI or doing upscaling, but is “running an experiment on select YouTube Shorts that uses machine learning to unblur, denoise and improve clarity (similar to what a modern smartphone does)”.

MHL first Pakistan biz in anti-piracy alliance

Pakistan's MHL (Merchant Holdings Limited) has joined anti-piracy group Alliance for Creativity and Entertainment (ACE). MHL will be the first ACE member company from Pakistan.

MHL is a licensed content distribution and broadcast services provider, delivering end-to-end broadcast and OTT services. It owns Begin, a subscription-based OTT platform offering Western entertainment and sports content to Pakistani audiences.

Photo metadata could include AI info

The IPTC Photo Metadata Working Group has proposed a draft set of properties for recording details of AI-generated images.

The suggested metadata fields would be added to the next version of the [IPTC Photo Metadata Standard](#) to be published in November of this year.

The [IPTC](#) is a global standards body for the news media. The Photo Metadata Standard is a widely used protocol for describing photos and is employed by news agencies, photographers, libraries, museums and other image-intensive sectors.

The new additions would address questions about what AI system or models were employed to generate an image and what original prompts or references were used as a starting point. The new properties would be AI Model, AI Text Prompt Description, AI Prompt Writer Name, and Reference Image(s).

The new descriptors would be optional, but the IPTC would recommend AI engines provide them when possible. Before being accepted, the properties must be approved by IPTC member organizations at the group's Autumn Meeting in October.

SMPTE study group for content authenticity

SMPTE (Society of Motion Picture and Television Engineers) has launched a Content Provenance and Authenticity (CPA) in Media Study Group. The project aims to catalog content provenance and authenticity tech, as well as identify allied work happening in other media industry professional organizations.

The group will make recommendations on how SMPTE can update standards or potentially create new ones for strengthening how media companies and consumers can confirm content authenticity and provenance. The study group plans to summarize its findings in future reports.

The study group includes SMPTE standards community representatives from Ross Video, Sony, Adobe, the European Broadcasting Union, and Metaglobe. It will be chaired by SMPTE Director of Standards Thomas Bause Mason.

"The CPA SG was established at a critical juncture, as artificial intelligence becomes increasingly integrated into media production," said Mason. "In this evolving landscape, ensuring that audiences can trust the authenticity of the content they consume is more important than ever."

Netflix gives partners an AI heads-up

Netflix has published guidance for its partners on Gen AI use in Netflix content. The post aims its partners understand when and how to use GenAI tools.

"We expect all production partners to share any intended use of Gen AI with their Netflix contact," it says, "especially as new tools continue to emerge with different capabilities and risks."

Read the full post [here](#).

Sony ups video authentication offerings

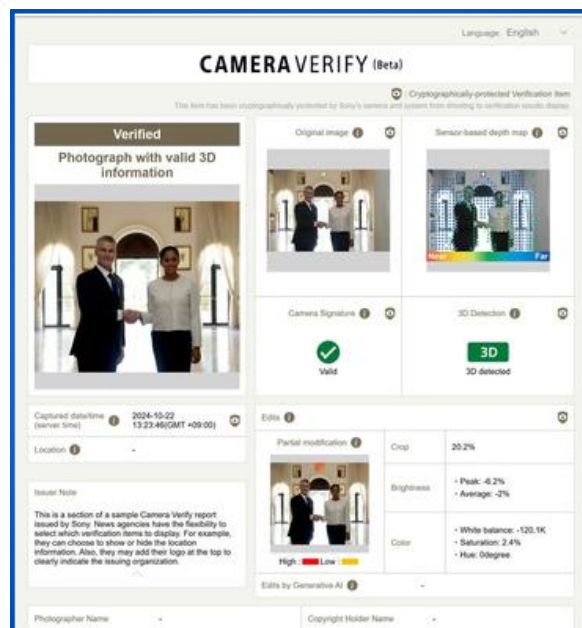
A new video camera from Sony, the PXW-Z300, claims to be the world's first camcorder with the ability to embed C2PA (Coalition for Content Provenance and Authenticity) metadata with the content it captures. C2PA is a metadata standard for tracking content provenance and is already available in Sony still cameras.

Designed for news and documentary shooters, the XDCAM camcorder features three 1/2-type 4K Exmor R CMOS sensors, AI-powered subject recognition and flexible LCD arm. The camera's full video authenticity functionality will require a separate upgrade license and will support MP4 only. The official release date is yet to be announced.



Sony has also released a beta version of Camera Verify, a new feature in its Camera Authenticity Solution, that enables sharing of image authenticity information via a dedicated URL. The Camera Authenticity Solution, designed for photojournalists and news agencies, embeds C2PA digital signatures and Sony's proprietary 3D depth information directly into the image at the moment of capture. News organisations can offer the URL for the Camera Verify report on their websites or in supporting materials to help support the authenticity of images.

Also newly available is the Digital Signature License, allowing the embedding of digital signatures directly into images captured with Sony cameras.



C2PA

returns to

IBC
C

This year's cohort of IBC Accelerator media tech projects includes a more focused look at applications for C2PA

The IBC Accelerator Media Innovation Program is an annual trial of media tech innovation convenes in months leading up to the [IBC Show](#), one of the world's biggest gatherings of media tech vendors. The Accelerator joins together media companies for experimentation with new media workflows, business models, and technology, then presents the results to the wider industry.

This year's Accelerator Projects include experiments in Gen AI content, AI production assistance, ultra-low latency video, private 5G networks for drones, and measuring the environmental impact of media workflows.

This cohort of projects also sees the return of a collaboration examining how the C2PA protocol might help fight disinformation.

Last year's C2PA project took a general look at how broadcasters could identify disinformation and help audiences source trustworthy news. This year iteration, "Stamping Your Content (C2PA Provenance)", strives for a clearer focus, with an aim to develop open source tools that enable organizations to integrate C2PA content credentials into their workflows.

"Last year's project was a very broad church," explains Mark Smith, IBC Council Chair and co-lead for the Accelerator program. "It focused on defining the wider challenges around combating misinformation, fake images and video, including content provenance, the value of available detection tools, and new approaches to collaboration. ➤"



shaping the future

12-15 Sept 2025, RAI Amsterdam
show.ibc.org



Register
now
for IBC2025

#IBC2025



RIST Forum

RIST: Secure. Reliable. Ready for Anything.

Live video delivery that stands up to piracy, cyber threats & network chaos.

The Reliable Internet Stream Transport (RIST) protocol is an open, interoperable standard for transporting live video over unmanaged networks.

Lock it down:

End-to-end encryption
and strong
authentication.

Keep it moving:

Packet recovery and
error correction for
rock-solid streams.

Play well:

Built by the industry, for
the industry –
interoperable by design.



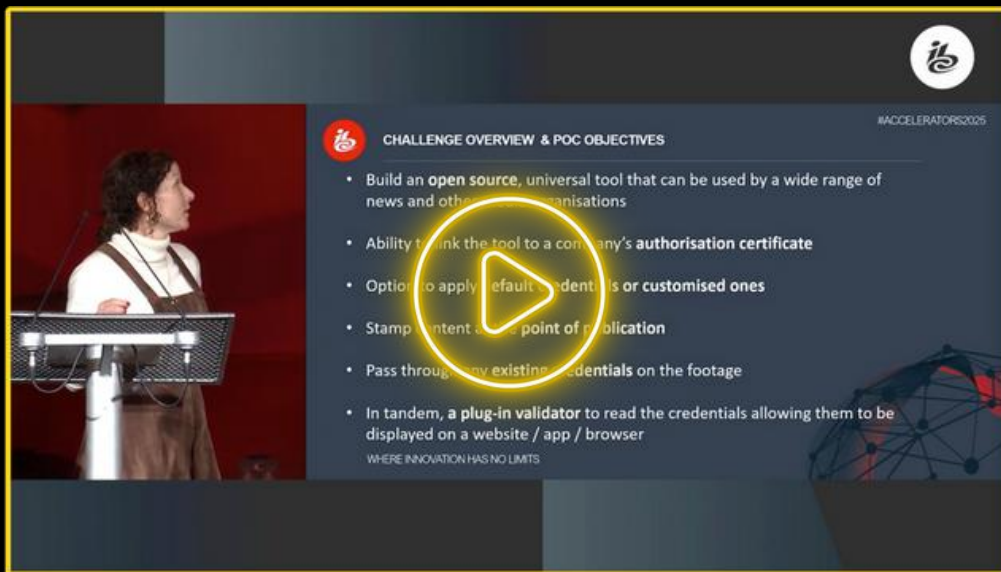
Used for:

- Professional media workflows
- News and sports contribution
- Remote production
- Affiliate and primary distribution

Protect your streams. Deliver with confidence.

Become a RIST Forum member

www.rist.tv



WATCH: A short overview of this year's C2PA IBC Accelerator Project from the Accelerator launch event this year

"Due to the enormous scale of the challenge we set out to explore, and of course, the limited timeframe, we only scratched the surface of this global problem. This year, we're laser-focused on a specific project track, helping organisations put new authentication methodologies into practice and integrate provenance tools into real-world workflows."

A FOCUSED TEAM

The IBC Accelerator projects are supervised by "Champions" usually broadcasters, standards bodies, and end users. This year's C2PA project includes as its Champions BBC, ITN, Yle, RTÉ, ITV, IET, EBU, AP, ASBU, Channel 4, and IPTC. The tech-provider participants include CastLabs, Videntifier, Media Cluster Norway, Open Origins, Trufo, TCS, and Sony.

The project was proposed by Judy Parnall, Principal Technologist with BBC R&D, and Tim Forrest, Head of News Production & Archive with ITN, both of whom were involved in last year's C2PA Accelerator.

Their goal will be to validate C2PA's readiness for real-world, multi-format deployments, while developing open assets and documentation that the industry can adopt and build on.

TOOLS FOR TRUTH

There is a feeling that the clock is ticking and that every year that goes by without adequate tools for fighting disinformation is a month lost for factuality.

"AI-generated content is becoming harder to detect," says Smith. "There's an urgent need for tools that can verify where media comes from and how, by whom, and to what extent it has been altered. By providing these tools and developing a comprehensive, concise workflow process through the project, we're aiming to give media organisations a framework to more effectively assert content authenticity."

The results of the Accelerator C2PA project will be unveiled during the IBC Show, September 12-15.

"There are some extra dimensions to the project that we hope to include in our demonstrations and showcase at IBC, but clearly we don't want to reveal all ahead of the show!" says Smith. "Some of the world's leading news organisations will be there to explain why this is so critical and their vision for what will hopefully become the open source stamping tool of choice by the world's newsrooms." 🟡

COORDINATE YOUR DEFENSES OR LOSE YOUR CONTENT

A multi-layered approach of intelligence-gathering and monitoring helps Friend MTS keep customers' content in the right hands

"There has never been more piracy. That is one of the biggest challenges that the industry faces," explains Robin Boldon, Head of Product at [Friend MTS](#).

"All the great content we have also means there more opportunity for pirates to get between rights holders and their audiences. And the days of politely sending a request to a service provider and keeping your fingers crossed that they will comply are long gone."

Criminal activity thrives when victims are in isolation. Rights holders, recognizing this, are beginning to collaborate

"It is seen as a more collective challenge," says Boldon. "Only a few years ago it was very much seen as the rights holders' problem."

MONITOR, IDENTIFY, DISRUPT

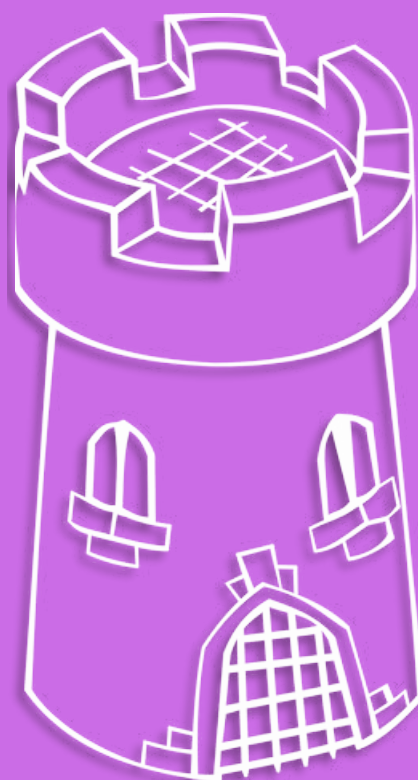
Friend MTS offers services to content owners with three main strategies of monitoring, identifying and disrupting. They help customers first identify who, where and what is being pirated by harvesting detailed data signals about each infringement. Knowing where to look is key and FMTS has built up a continuously updated "piracy source register", a database of verified sources of online piracy.

These collected signals are then run through multiple analytics processes, from complex automated pattern recognition to expert human analysis, to look for various indicators that pirates may not even be aware they're divulging. Once the suspected content is identified, video evidence can be extracted,

and Friend MTS's proprietary video fingerprinting technology is used to match it with a known reference provided by the rights holder.

Obviously, this is a highly complicated, carefully orchestrated series of interventions. How long does it take to track down and process any one pirated video? Weeks? Days? Hours? Minutes?

"The process scales up," says Boldon. "We're actually processing more than three years worth of video every day. And this is all working in real time. To be effective, every second counts"



Disrupting the pirates includes everything from the aforementioned request to the service provider, but also intervening in the web of referrers and aggregators that point users toward the pirated content.

Tools also include domain and dynamic server blocking which can compel local ISPs to block access to verified forms of piracy with the ability to continuously update the location of the pirate's infrastructure, avoiding the need to having to treat every new domain or IP address the pirate uses as a different legal application to a court or regulator.

Forensic watermarking, embedded when the content is first published, also allows for more precise identification of exactly where, when and how the content was first stolen.

"Rights holders are then able to take action while it's happening. For a high-value sporting event, your success is measured in minutes, so it's important to have these orchestrated approaches."

But content doesn't need to be a live sports final to demand the same kind of rapid response. A day-and-date release of scripted content can be subject to the same instantaneous attempts at piracy as a live event. Major damage can be done within hours or minute of the drop.

COORDINATION, NOT WHACK-A-MOLE

The best strategies for dealing with piracy are coordinated layers of defense and offense. If you're playing whack a mole, chasing down potential offenders only as they pop up, you're missing a lot of them, and wasting resources.

"The response is to be precise. Precision comes from your ability to capture the data around the different forms piracy and look for patterns. Our customers will have their own data points for legitimate content consumption, then when we can show them patterns that fall outside that, together we can build up a picture of the threats causing the most harm to their business."

Good coordination includes not just the tech, but communication and intelligence-sharing between organizations. Friend MTS is regularly engaged in investigation and

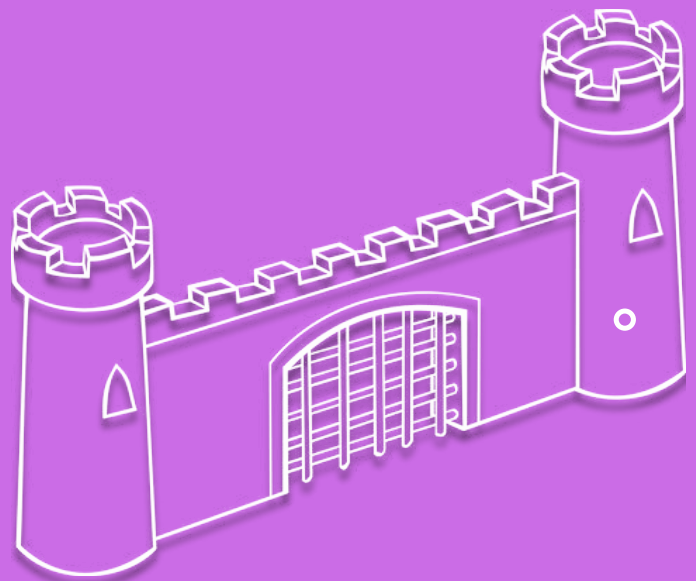
and intelligence gathering, which helps them predict where and how content theft is likely to happen, particularly for major broadcast events, like the World Cup. This means they can even put potential offenders on notice before they strike.

"What we've found is that in certain situations, being proactive with some hosting providers yields better results. Rather than it being a tip-off that we're onto them, they will comply, because they don't want the negative publicity. But it still must be part of an overall multi-layered strategy."

Fighting cybercrime is always an arms race. New techniques are regularly being hatched by agile and often well-funded criminal organizations for whom content piracy might only be one of a number of illegal revenue streams.

CDN leeching caught the industry on the back foot a couple years ago, but now thanks to robust investigation and knowledge sharing, a next generation of protection is being developed.

"In industry working groups and trade bodies, we're seeing a more collaborative attitude between rights holders and licensees, with rights holders and partners talking more collectively about where insight can be shared and best practice can come into play."



IP PREDATORS

THE TECH ARMS RACE AGAINST PACKS OF PIRATES

By Neal Romanek

Content piracy is happening worldwide on an industrial scale. Protecting copyright is a battle that never ends

“What we see is increasingly connected to organized crime,” said Miruna Herovanu, Executive Director of the AAPA, at iAU!’s Content & IP Defense Summit in June about the ever-growing threat of content piracy. “It’s an organized network that takes place in many countries.”

The AAPA (Audiovisual Anti-Piracy Alliance) is an EU organization fighting piracy through lobbying, law enforcement, and partnerships. Its working groups focus on hosting infrastructure, social media, artificial intelligence, and piracy disruption. Members include Canal+ Group, beIN Sports, DAZN, the Premier League and Sky, plus tech providers like Friend MTS, Irdeto, Verimatrix and Synamedia.

In 2022, an AAPA study, "[The impact of illicit IPTV in Europe](#)" calculated that in the previous year, rights holders in the EU and UK lost €3.21 billion to IPTV piracy alone, while pirates made €1.1 billion in revenue. The report also estimated that in 2021, 4.5% of the EU/UK population used illicit IPTV services. Users of those services spent, on average, a bargain €5.22 per month.

Herovanu has worked in European trade associations and regulators her entire career, with a special focus on intellectual property and copyright. She sees education as an important part of the AAPA's strategy.

Pirates are often legally as well as technologically sophisticated, taking advantage of the differences in legal frameworks across countries to circumvent some copyright regulations.

"Also there's the training of law enforcement on the specificities of these crimes, which are very technical and complicated. And there are different legal regimes, because copyright is territorial."

Earlier this year a [report](#) published by Enders Analysis accused the big tech companies of doing little to curb what it dubbed "industrial scale theft of video services".

Authored by Enders' [Gareth Sutcliffe](#) and [Ollie Meir](#), the report focused on the European market and claimed that easy discovery and access of illegal services, often through simple hardware like the Amazon Fire Stick,



have turned the digital content ecosystem into an open bank vault for pirates. The problem has been worsened by a lack of engagement from Google, Microsoft and the other big tech companies.



CONTENT PROTECTION REQUIRES STRONG TECH

Technology infrastructure for video delivery is both the first defense and the first big vulnerability when it comes to content piracy. Failures at this level can mean disaster for content owners and their bottom lines.

"We deal with tier one broadcasters and live transmission. The content we are managing is critical, with ads that are worth millions of dollars," said [Sergio Ammirata, PhD](#), Founder and Chief Scientist at SipRadius and Director of [RIST Forum](#).

SipRadius specializes in software-defined video delivery systems, with military-grade security. It has also developed a custom operating system, called CoralOS, to avoid reliance on general-purpose systems and the vulnerabilities they might bring.

The RIST protocol, whose supporters include tech providers like AWS, Zixi and Cobalt, in addition to SipRadius, is an interoperable standard for transmission of live streams that includes features like 256 bit AES encryption and rotating keys. The protocol is designed to prevent data interception.

"The level of anxiety about losing control of content is very high," said Ammirata. "It took ➡



WATCH: At the ¡AU! Content & IP Defense Summit, we discuss the ongoing battle against packs of content pirates

a year's worth of security audits to allow our CoralOS to transmit live streams."

There is a continual arms race in content safety, with pirates sooner or later finding ways to get around new technologies. Different approaches are required for live delivery versus OTT or on-demand. While the protection of live content can often be managed by the latest delivery technologies, OTT relies more on a wider distribution network that is upgraded only gradually.

"With OTT, you are working with technologies that are three, four or five years old, which have already been exploited and that's where the breaches come."

OPEN OR CLOSED, YOU'RE VULNERABLE

Ammirata's experience heading up the RIST Forum, which promotes an open source, open-specification video transport protocol, has attuned him to tradeoffs between easy universally accessible tools and security needs. The transparency of open source tools means hackers know what the vulnerabilities are upfront—and can exploit them.

"Open source, by itself, isn't necessarily secure," he told the Summit. "It's up to the

implementor to harden it. A lot of times you see open source workflows, but they haven't closed the holes in them. Or they did close the holes but did it years ago in the first version of the application, and they haven't kept up with the updates."

Continuously upgrading and patching software, open source or not, is just good hygiene when it comes to preventing attacks. But open source software, because of generally slower development times, suffers from a longer updates cycles.

Closed-source software, which does not have the public-facing record of updates, vulnerabilities or versioning, is generally assumed to be more hacker resistant. But this is based on "security by obscurity," assuming that because you've concealed how you're system works, it will automatically be safer. Not revealing your secrets to potential criminals is good sense, but in some instances it may just be the digital equivalent of hiding your front door key under the welcome mat. And there are numerous closed-source systems that are far more vulnerable than open source implementations.

As is often so, it comes back to the diligence of the people involved. Closed-source

software brings no automatic security guarantee with it and can just as easily hide vulnerabilities from customers as hackers.

"In the past, with closed source operating systems, we have seen holes that have been open for years and years with hackers still exploiting them."

WINNING BY CHANGING THE RULES

With content distribution now a part of almost every business, security and anti-piracy needs to be part of every business plan. Frequently, content is now sent directly to fans and subscribers without passing through a broadcaster or a distributor.

New ways of thinking about content distribution, create new attack surfaces for pirates, but also new opportunities for protecting rights and IP.

Eluvio's "Content Fabric" is a decentralized distribution and storage network which incorporates blockchain technology to identify participants, nodes, and content across the infrastructure. The company is headed—and was co-founded by—[Michelle Munson](#), who created the FASP (Fast Adaptive and Secure Protocol) technology that launched video transfer workhorse Aspera, now part of IBM.

Multiple sports leagues are using Eluvio's Content Fabric to connect to their audiences. While the user experience of both the content owner and audience might be indistinguishable from a traditional CDN distribution, behind the scenes there is an entirely different process at work. Rather than content or its stream being duplicated across locations and CDN's, the Content Fabric is in effect retaining only a single instance of content which is being accessed directly by those with authorization.

This could be a valuable tool for combatting ploys like CDN leeching, a new piracy strategy which directly accesses content hosted on a Content Delivery Network without proper authorization. In the case of the Content Fabric, there are no duplicates of content spread out across CDNs.



The Content Fabric also enables direct gatekeeping of content by the rights holder. They can control ticketing and content access without going through a third party service for monetization or fan interaction. Reducing the number of third parties entering the chain, also means getting more direct audience and viewing metrics.

Says Munson: "Video over IP distribution has been broken up between the source, transcoding, packaging, the origin, and the CDN, with other providers sitting on top. It's been difficult to create the end to end context.

"The byproduct of our end-to-end session-based security, that's owner controlled, is the audience relationship and associated data are direct."

"Unfortunately, the law really runs behind these types of behaviors."

Miruna Herovanu



Eluvio also offers security for contribution in the production workflows with the Content Fabric providing end-to-end encryption, forensic watermarking in line, and options for visible, dynamic watermarking and owner-controlled security.

"Camera feeds need to go to a variety of destinations for remote production," explains Munson. "For that we need low latency, but with encryption end-to-end. We need to distribute that in a way that guarantees authenticity and ownership, and guarantees that there can be no piracy. ➡"



"If you look at security, you see everything is encrypted based on the owner's keys. We've been involved in a successful major pilot this summer with one of the biggest leagues in the world. Those sessions are under their control, end-to-end."

CLAIMING WHAT'S YOURS

Dr. Manny Ahmed, founder of OpenOrigins and a researcher at the University of Cambridge, has been tackling the content control problem from the point of view of content provability, particularly important in a world of material influenced by AI. Authenticating provenance of content at its source is a key part of the OpenOrigins toolkit and includes authenticating pre-existing IP libraries.

"There is a lot of attention focused on content that is being created now or in the future, but no one was thinking in depth about what we do with all this historical content," said Ahmed.

"How do we know that your version of Obama's speech from 2008 is the real one, when we could create an alternative version that looks just as photorealistic?"

Organizations like C2PA are working on methodologies to certify the provenance of content, but these still rely ultimately on the authority of a specific organization of individual. OpenOrigins aims for a solution for content authentication that is decentralized that doesn't have to refer to gatekeepers or nodes of authority.


"I think C2PA is fine if you are working within a very limited information silo," noted Ahmed. "If you are in an organization and you have end to end control over what software everyone is using. But the moment you put it on Twitter and someone takes a screenshot, the metadata gets ripped out. You have similar issues with water-

marking, which is always going to be an arms race."

With OpenOrigins, blockchain is used to store proof information as content is ingested. The company's Archive Anchor, which builds a provenance layer into media assets, has already secured over a petabyte of historic news content from media organizations like ITN.

"We work with large news archives," said Ahmed. "We do a security audit, then literally go item by item and provide an audit trail of when that piece of content was first uploaded, how it was modified, and how it was broadcast. Any further modifications are being tracked as well."

Despite the development of new tools, it's important to keep in mind that the



landscape is not static. The media tech environment today is different from the one even six months ago.

"Pirates adapt quickly. They are the first ones to make use of technology," warned Herovanu. "And unfortunately, the law really runs behind these types of behaviors."

The world of IPTV has been one the newest targets, but wherever there is content, there is vulnerability.

"So far tech companies and hosting services have benefited from a lack of responsibility. But if there was some common recognition of the social and moral duty that these intermediaries—some of whom are offshore—whose infrastructures are being used by pirates that would help.

"In the EU the bigger actors, such as Meta and X, have to take measures to remove illegal content from their services, but that's not enough because pirates are obviously very resourceful." 🟡

C2PA IS NOT A PROTOCOL DROID:

It's a plan for restoring freedom to the content galaxy...

By Neal Romanek

The C2PA standard is getting wider adoption to help media professionals— and audiences— tell fact from falsehood



If you see a photo of people burning a car, and the caption reads “Rebels riot in the city center”, odds are you will accept the description at face value—even if those in the photo were not rebels, and it was actually taken a long time ago, in a city far away.

We are inundated by so many images daily, we rarely stop to question where they came from. On the rare occasion we do try to track down the provenance of an image, it can take some real detective work to find the source.

WHAT IS C2PA?

C2PA – the Coalition for Content Provenance and Authenticity is a media industry body developing global protocols for tracing the provenance of digital media.

The resulting C2PA metadata standard enables creators, publishers, and consumers to verify where a piece of content was created and what changes it went through on its journey to appearing on-screen. The C2PA standard doesn't pass judgement on the veracity of an image. It just gives you the facts about where it came from.

As with the introduction of any new standard, progress is gradual, with incremental adoption and sudden innovation happening simultaneously. Camera manufacturers are beginning to implement C2PA support in their gear. Sony for example has released its new PXW-Z300, which it is touting as the first camcorder to support C2PA for video.

“In my opinion, for C2PA to succeed as a standard, it needs to be widely adopted and implemented,” explained Felipe Dana to iAU's Content & IP Defense Summit this summer. Dana is General Manager for Field

Innovation at the Associated Press. He is also a veteran photojournalist and winner of a 2023 Pulitzer Prize for Breaking News Photography as part of AP's coverage of the invasion of Ukraine.

"When you go to the pharmacy and buy medicine, you expect it to be sealed," Dana said. "Hopefully, in the future, when you see an image, you're going to expect it to be 'sealed' so you can see where it came from and can track the provenance of it."

ARE WORKFLOWS READY FOR C2PA YET?

The ideal of being able to track provenance "glass-to-glass" — at every step, from capture through to its appearance onscreen — requires wide interoperability

among workflows, asset management systems, and CMS's. At this point, there aren't any examples of a perfect glass-to-glass implementation, but proofs of concept are starting to sprout up. The first wide use case of C2PA is likely to be the stamping of content at the point of publication.

Helge O. Svela, CEO of Media Cluster Norway explained to the Content & IP Defense Summit that this use of C2PA by the publisher is a leap forward for encouraging trust and integrity in media outlets. It means a broadcaster or news organization is stepping forward to endorse the authenticity and provenance of its content.

"Even if there's not a perfect chain going all the way from

camera, to the MAM system, to the CMSs, and out to the published article, I think we're going to see publishers asserting that, yes, this image is being published by, let's say, the NRK News, and it was taken in Ukraine, and we at NRK put our reputation on the line saying so."

But the real value of C2PA use may appear more in the breach than the observance.

With the internet on the verge of being overcome by Gen AI slop, those organizations who can demonstrate where an image came from will have an advantage over those who can only say "trust us" — or worse, "we don't know".

"Instead of trying to control the noise, we have to try to control the signal, by ➡



WATCH: Our panel at the jAU! Content & IP Defense Summit discusses the present and future uses for C2PA

adding provenance to the trustworthy content of real newsrooms with real images,” said Svela. “That’s the way for the signal of good content to stand out from all this noise.”

Media Cluster Norway is host to Project Reynir, a group focusing on tech solutions to threats from disinformation and Gen AI. C2PA is at the forefront of the agenda. The organization’s stretch goal is to get 80% adoption of C2PA in Norway’s news ecosystem by the end of 2026.

While it feels like we are in an factuality emergency and there is an urge to deploy any and all potential defenses immediately, the transition to C2PA and other forms of media authentication really is just a logical evolution in developing a more secure, trustworthy, and useful information space.

to HTTPS’. We used to text, but then decided we needed encryption and moved to signal and WhatsApp. Think of current image metadata, like EXIF, as like the unencrypted version, and CTPA is adding encryption and security on top of that.”

One of The Guardian Project’s major contributions to content provenance is Proofmode, which is an open source stack of software tools, including an Android and iPhone app, for establishing the provenance of content at capture.

“Early in our work we realized that smart phones are also smart cameras, and we started building provenance and authentication tech,” said Freitas. “There is a concept in US federal law of ‘self-authenticating evidence’, evidence that comes packaged with digital

Norwegian post-production software company Cutting Room, also part of Project Reynir, has incorporated the Proofmode SDK into its iOS, allowing teams to capture broadcast grade video with C2PA credentials built in which can be send directly to the cloud for editing.

“Our code has been adopted by everyone from Signal and the Tor project to WeChat and Grindr.”

AUTHENTICATION IN TIME OF WAR

Freitas’s team worked with The Starling Lab for Data Integrity, which prototypes data authentication tools for journalists, historians and legal professionals, as well as Stanford University, to help authenticate content collected from Ukraine.

“Using the Proofmode app and a prototype version of Signal that had Proofmode built in, you could capture the evidence on the ground in Kharkiv. It would submit over Signal and get stamped again by a server process. That would then go into an evidence chain, eventually submitted to the ICC (International Criminal Court). And in ten years, when justice is sought, we’ll be able to rely on that.”

While the media industry is working to bring C2PA into regular workflows, it could very well be adoption by the general public that helps it achieve critical mass, especially once the language of content provenance becomes part of the everyday discourse around what we produce and consume on our personal devices.

“Instead of trying to control the noise, we have to try to control the signal”

Helge O. Svela



PROOFMODE AND HUMAN-CENTRIC SOFTWARE

Nathan Freitas founded The Guardian Project, which works to build free, open source software for human rights and humanitarian applications. He likens C2PA adoption to any of the other security upgrades that are a daily part of work in digital media:

“The web used to be HTTP, but then we said ‘let’s move

signatures and notarizations, so you don’t have to go through a whole forensic process to see if it was manipulated.”

Proofmode originally relied on its own standard, but seeing the benefits of mass adoption of a widely recognized protocol, its focus switched to C2PA. The work that Proofmode has piloted is now publicly available through an SDK, backed by major media tech providers.

Determining who took a photo from an event on the other side of the world may not interest everybody, but being able to know whether an image of a person you're flirting with on a dating app is real—and up to date—is something that a lot of people can get behind.

"Grindr are very progressive in thinking about unique security threats," said Freitas, "especially since some of their users are in places in the world that are not very safe for them. You never know who the champions of important new tech will be."

The real test of content authentication standards like C2PA won't be whether they improve the work of publishers and news outlets—although that's extremely important right now—but how they improve the lives of everybody who accesses digital content. ●



JUNE 31, 1984

ON THE TRAIL OF THE GHOST INFLUENCERS

Journalist Rob Waugh cracked open a whole world of widely quoted, but nonexistent, experts. How do real human experts get heard in an ecosystem that reward fast fakes?

“ I was approached by a guest blogger,” recalls Rob Waugh. “But there were no traces of that person on the internet, just dead ends. I thought: This person doesn’t exist.”

That was the unsettling moment that started UK tech journalist Waugh on his ongoing investigations into a world where nonexistent experts are making PR agencies and publishers real money.

His breakthrough was the discovery of a second “ghost influencer” when he sent out a call for a psychologist who could give an opinion for an article he was writing — ironically as it turned out — on the impact of identify theft.

One of those who responded, called Barbara Santini, had already been quoted numerous times in major media publications, including *Vogue*, *Cosmopolitan*, and UK papers *The Sun*, *The Daily Mail*, and *Metro*.

But when Waugh began browsing through Santini’s credentials, he was surprised to find that, despite her claiming a master’s degree in Psychology, Philosophy and Linguistics from University of Oxford, the only verifiable links to any professional work were with online sex shop Peaches and Screams and some CBD brands. The photo pictured here was used across that handful of profiles.

There were other things that seemed suspicious to Waugh: “Real psychologists don’t respond to people two minutes after a request with twelve carefully crafted paragraphs of copy.”



Unreal genius: This is the photo ascribed to ‘Barbara Santini’. But Barbara Santini doesn’t seem to exist.

Santini’s bio at *Peaches and Screams* paints a vivid picture of someone “on a mission to make sex advice as accessible as a good cup of tea and to shatter taboos across all cultural corners. When she’s not busy revolutionizing the way we talk about sex, Barbara’s diving into her delightfully eccentric hobbies. She floats her way through yoga classes (yes, on water!), hunts down the most fabulous vintage fashion finds, and loves cracking the codes in escape rooms.”

Digging deeper, Waugh began to suspect that Santini, not only wasn't an Oxford-educated psychologist, but that she wasn't a real person. Looking at her writing samples, he spotted clues that her content could be the creation of AI. Writing subheads in title-case was one subtle peculiarity. It's a US stylistic standard, and one that a professional UK journalist would be unlikely to use (UK style favors sentence-case). For a chatbot like Chat GPT, trained on American content, it would be fairly typical output.

Santini's insights and quotes appeared in lifestyle pieces that covered a spectrum of topics—"Cringey or cute?: Top couples' pet names revealed" or "The signs you're primarily attracted to intelligence over looks – and why it can be considered controversial" or "What happens if you don't cry? Is stopping tears bad?"

"Santini would comment on anything," says Waugh. "She can create comments instantly, using ChatGPT, because she doesn't exist."

Waugh finally tracked down the home base for Barbara Santini's expertise.

"I looked into who owned the company that she worked for. I realized that Barbara Santini was actually two Lithuanian men who owned a chain of CBD brands and sex shops and who, I believe, employed a blogger in Nairobi who sent out the copy by email."

THE FAKE INDUSTRIAL COMPLEX

Waugh flagged the fake to the referral service ResponseSource, an agency connecting media outlets with experts and sources for almost every topic imaginable. Services like ResponseSource will often get their expert sources through PR agencies, rarely with diligent vetting of the experts put forward. As long as the PR agency pays its bill, few questions are asked.

"ResponseSource said 'We've given the person a final warning.'" Waugh laughs. "Why have they given them a final warning? The person doesn't exist."

In partnership with Press Gazette, Waugh published a full investigation into the Santini hoax and others. For the piece, Press Gazette tried to contact Santini directly and were threatened with legal action if they continued to pursue the matter—followed then by complete silence. The piece resulted in embarrassed mainstream media outlets quickly pulling their Barbara Santini content or issuing retractions.

With his eyes opened to telltale signs of non-humanity in journalism, Waugh began to spot other fake contributors. Looking for expert input for an environmental piece he was working on, he encountered a thought leader whose background included no verifiable expertise and different bio pictures on things she had written.



"To me this is a story about journalistic ethics. It's about people attempting to fool news outlets. But I realized that for other people it's a purely technical issue. The people who do this are SEO guys, and what they are trying to do is boost EEAT, a method Google uses to rank sites based on the expertise they have represented. If your site is associated with a widely cited expert, or publication, you can boost its ranking."

Within the SEO industry, the creation of fake contributors is now incentivized to the point. It is much more common than most readers would guess.

MONEY FOR NOTHING

Waugh has since "gone down a rabbit hole," as he puts it, into an ongoing investigation of the fake expert phenomenon and has encountered new methods companies are using to ➤

JUNE 31, 1984

generate fake expert content, that make the idea of individual ghost influencer seem quaint. Now there are networks that produce thousands of AI-generated publications which, from server to screen, never pass through a human being.

"They spew news 24/7 with the goal of getting onto Google Discover. Some of the people who operate these have become millionaires. These fake publications are outranking real ones staffed by human journalists."

Some news outlets are tightening up the verification process for experts, although it often falls on individual journalists to do the actual

legwork. Yahoo News, for example, now requires two kinds of ID verification for any expert a freelancer quotes in a piece.

News networks have also sent out warnings for journalists not to automatically trust experts provided by services like ResponseSource, where their identity cannot be independently verified. ResponseSource is also reportedly upgrading its protocols for expert authenticity.

In a world where content can be monetized by consistently hitting certain algorithmic targets at scale, these fixes still duck the main problem of a system that rewards

dumping hard-won, but time-consuming and expensive, human expertise.

"The time pressure on journalists to deliver yards and yards in increasingly less time of copy for increasingly less money means we're more vulnerable.

"The financial motivation for doing this is extremely real. And journalists are going to deal with more and more fake people." ●



WATCH: Rob Waugh tracked down the wildly quoted—but fake—influencer Barbara Santini to two Lithuanian businessmen.

IAU!

AU-WORKS.COM

**CLICK TO
GET THE NEWSLETTER**



iAU!



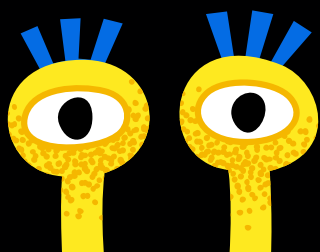
MONSTER LAB

**iAU!'S NEW EVENT SERIES,
WHERE CREATORS HONE THEIR SKILLS
BY STUDYING BAD GUYS...FICTIONAL & OTHERWISE**



**HATCHES
OCTOBER 18**

**FOR TICKETS & INFO GO TO
AU-WORKS/MONSTERLAB**



CONTENT BY NO ONE, FOR NO ONE: Surviving the Gen AI bubble

*Can the media & entertainment put the brakes
on its toxic relationship with Gen AI?*

"The creative spirit of humanity is an incredibly important thing. And we want to build tools that lift that up, that make it so new people can create better art—better content, write better novels that we all enjoy. I do believe that humans will be at the center of that."

"I also believe that we need to figure out some sort of new model on the economics of creative output. I think there are incredible new business models that we and others are excited to explore..."

Thus spoke Sam Altman, CEO of OpenAI at TED early this year.

The interview has been watched 1.7 million times at this writing.

OpenAI, you will recall, is a company founded by Sam Altman, Elon Musk and other online technology experts in 2015 "with the goal of building safe and beneficial artificial general intelligence for the benefit of humanity."

The OpenAI founders are all pretty smart people. Neither Sam Altman nor OpenAI President Greg Brockman graduated from university, which is certainly evidence of just how smart they are. Smart people graduate from Stanford. Really, really smart people drop out. Apparently.

Brockman actually dropped out of two elite universities, so that may make him some extra extra smart.

In 2023, Altman and Brockman also both dropped out of their own company when they were offered a sweet deal to leave OpenAI for a new AI team at Microsoft. The two were quickly lured back to their alma mater by shareholders where they remain, for now.

It would be churlish not to admit that Gen AI has positive qualities. But fidelity and integrity are not among them.

AI gives the appearance of performing great feats mostly because we can't see what goes on behind the scenes. We can't see what's happening in the kitchen.

So here is a quick recap of how your favorite Gen AI tool actually works (spoiler: there is no kitchen): ... ➤

HOW GEN AI ACTUALLY WORKS

Gen AI works like a wacky restaurant from a Dr. Seuss story.

Imagine you're sitting at your eat-a-ma-thing. You type out what you would like to eat. You describe it in detail.

What then happens is your fancy robot waiter zips downstairs into a deep vault containing every imaginable thing that could be eaten.

The owners of the restaurant have travelled the world and stolen every version of every sandwich and pie and salad and crab fried rice and stored them in a temperature-controlled facility as big as Ireland.

Speeding through the vault, your robot waiter picks a meal off the shelf which looks closest to the meal you described. It zips back up to the restaurant and presents that meal to you.

You are delighted. You say "My compliments to the chef. He's a genius. Just like Sam Altman."

Of course the chef is not a genius. There is no chef. There is only a vault filled with every meal that anyone has ever made.

You decide you would like your meal with pepper on it. But the robot waiter doesn't add pepper. What it does is zip back down to the vault and find a version of your meal with pepper on it, which has also been waiting in the vault, all this time, ready to go.

If you would like even more pepper, the robot waiter does not add even more pepper. It goes back and finds yet another version of the meal, with even more pepper, that has also been stored in the vault all this time.

If you decide you want to add ice cream, the waiter doesn't go and retrieve ice cream. It goes and retrieves the version of your meal (with the extra extra pepper) with ice cream this time

The reason your waiter can bring back your meal so quickly is it uses a jetpack powered by truffula trees.

Alright, so Gen AI doesn't actually work like that. And, yes, actually Gen AI does actually work like that.

The main point to ingest here is that in order for it to appear that a chatbot is catering casually to your every whim, it has had to steal and store an awful lot of versions of an awful lot of meals and use an awful lot of natural resources to give you the impression that it's serving you on the fly, and to ensure you give the restaurant a five star review.

It doesn't always get it right. When you ask for KFC, you can always tell there are only 8 or 9 secret herbs and spices in there.

STOLEN PROPERTY

"In my first encounter with generative AI, my feelings were that this is magical. How on Earth does it work?" said Gen AI expert Graham Lovelace to the IAU! Content & IP Defense Summit. Lovelace has become a top analyst on the effects of Gen AI on the media and entertainment sector.

"Then it very quickly turned to 'This is going to take everyone's job'. The more I looked into it, the more angry I became. It quickly became apparent— which we all know now—that the large language models behind the well known chatbots have been trained on stolen material."

Our Content & IP Defense Summit looked at the traditional culprits in content theft— pirates and hackers—but there is a new genus of content thieves operating globally.

They are the biggest content pirates in history.

And governments seem to be falling over themselves to collaborate with them.

"They have been trained on the world's intellectual property," Lovelace said. "They have scooped up that IP without consent, without any offer of compensation, and now in an act of organized crime, are creating the most capitalized companies on Earth ever. And yet the content creator industry is now going through some very, very hard times."



Sam Altman has yet to graduate from university

THE AI THREATS

Lovelace explained to the Summit that the threats that AI poses to content businesses fall roughly into three main categories:

I. EROSION OF TRUST

The ability for anyone, anywhere to instantaneously produce highly convincing text, image, audio and video content interferes with our ability to tell what is true.

Gen AI content can be very convincing—you could say its primary purpose is to be convincing. Even when we intellectually know what we're seeing isn't true, our brain still may still register it as a real event, something we have an opinion and feelings about. Remember the clip of Volodymyr Zelensky knocking out Donald Trump with a right hook—and the subsequent surge of well-being one felt?

We react to what we see viscerally, before the rational mind can step in to explain that what we've seen isn't real.

Knowing this, and knowing that realistic AI imagery is running loose in the media ecosystem, we may start to experience doubt about what we see. Even blatantly obvious attempts to fool people can do a lot of damage before they are debunked

The week of this writing, a deep fake video of Alexandria Ocasio-Cortez, in which she appeared to criticize to absurd extremes a controversial American Eagle jeans ad, was amplified by television host Chris Cuomo. On social media, Cuomo used the video, which he thought was real, as an opportunity to attack AOC.

Cuomo was ridiculed online, by AOC among others, for falling for the deep fake. He delivered an apology on his show, which included: "I was wrong...but what is right?"

With deep fakes and AI generated content becoming part of regular discourse, it becomes equally easy to ridicule genuine footage as fake AI content. The technique of labelling your opponents assertions as a hoax or "fake news" is already in regular use now. When the ➤



WATCH: Graham Lovelace describes the threats AI poses to copyright holders at iAU!'s Content & IP Defense Summit

pervasive attitude becomes “who knows what’s real anyway”; social contracts, democracies, and even markets start to weaken.

Untrustworthiness is built into the DNA of Gen AI itself. The purpose of Gen AI is not to deliver something true, but to deliver something you feel to be true. A chatbot’s entire goal is to make you satisfied with its response.

“The technology can’t help but give you an answer to a question,” Lovelace said. “No chatbot will ever say ‘I don’t know the answer to that.’ They will always have a go, based on the corpus of data they’ve been trained on, and try to infer an answer.”

II. DAMAGE TO INTEGRITY

When companies use AI to create content they might be playing with fire as far as brand integrity and public image are concerned.

The point that needs to be stressed repeatedly is that Gen AI is designed to satisfy. And it’s easy for us to confuse feeling satisfied with getting the truth. Fun fact: The truth often leaves us feeling unsatisfied and uncomfortable. If you’re feeling satisfied all the time, you may not be getting enough truth in your diet.

Every week there is a new example of AI making someone look ridiculous.

One recent AI self-own was perpetrated by Vogue, a brand which has spent decades honing an image of quality, exclusivity, and elite glamour. But for an internet moment this summer, they are a laughing stock—along with their advertiser Guess—for running an ad featuring an AI-generated model.

Unrealistic body proportions have been a staple of fashion since ancient times. The fact that the photorealistic model in the ad is about 10 heads tall, though weird, is in keeping with tradition. The laughable part is the rest of its anatomy which includes a unnerving mermaid-like waist, a suggestion of more than two legs beneath the dress, arms of different lengths, and a gigantic hand that looks like it should be covering John Hurt’s face.

At a glance, most people are convinced by the ad. Their eyes take in the image, and their brain says “Yep, an attractive woman.”

But designers, brands, and others who know quality—Vogue advertisers, for example—will care.

“No chatbot will ever say ‘I don’t know the answer to that.’”

Graham Lovelace



Vogue’s brand is about adorning real human bodies. While AI is a tool to make it easier to avoid human bodies—with all their whining and their need for money, food, and time.

The AI fashion company commissioned by Vogue, Seraphinne Vallora, is run by two London architects. Their website says “We want to harness the incredible power of AI to revolutionize marketing images. We realized that AI offered a hassle-free path to design brilliance.”

The company has created AI campaigns for Elle, Grazie, WSJ and the Financial Times.

Of course, we only have the word of Seraphinne Vallora that this is an entirely original AI creation. The training data is likely to remain forever obscure. Could it be, in part, based on the likenesses of real people? When you use Gen AI, you are exposing yourself to potential lawsuits later.

Lovelace explains: “We will very soon have some massive scandals where we see the interior of people’s homes or

hear things that have been said in private moments which will appear for everyone to see because of what these have been trained on. Identifiable images of our children will start to be available.”

III. FINANCIAL INSTABILITY

As a “disruptor” technology, AI is luring media companies into jettisoning current business models, perhaps without thinking through the consequences.

In a very short time, Google has ceased to be useful as a search engine, with its AI having been pushed forward to answer questions directly—based on other people’s content—to keep you from clicking out of the main Google search page.

“News publishers in particular are dependent on search for between 30% and half of their traffic,” says Lovelace. “Now AI scrapes those publishers’ content to create AI-generated snippets. They would argue that they provide the links and citations, but it’s clearly the aim of the developers to keep you in the Google AI overview environment.”

ChatGPT Search, Perplexity and other tech companies are exploring the same model. Why be a gateway to other information sources,

when you can scrape those sources and become the sole destination yourself?

AI is often touted as a way for smaller companies to do more with less, a tool to empower and rejuvenate a variety of sectors. This doesn’t appear to be the case with news and media production. In fact, it’s still unknown how much AI can add to the bottom line.

Right now, companies are laying off staff—or dismantling government departments—based on the projection that AI will be able to take over those jobs much more efficiently. But these decisions are based on virtually zero real world data. IBM boldly laid off thousands of employees, assuming AI would somehow take over their jobs, and ended up hiring almost as many back.

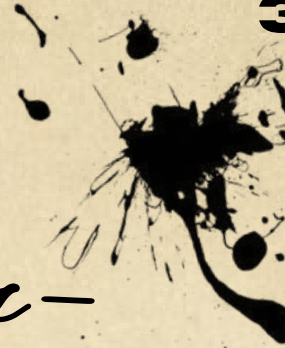
Big changes in tech generally fuel changes in society. A historian of Europe will tell you that the printing press helped launch religious wars which killed millions of people. One difference between AI and the printing press though is the printing press reproduced information faithfully.

Gen AI can create an infinite amount of content, but for whom and for what reason is an unanswered question.

Are billions of dollars that could be funding local news, journalism schools, arts education for kids, performance venues, and community media ultimately being spent on infrastructure to create content by no one, for no one, for no useful purpose? 🟡



Governments are abandoning creators— Something has to give



By Graham Lovelace, Writer & AI Strategist

*When things go wrong, we turn to our leaders for action—
we don't expect them to look the other way*

Humans are social creatures, though some of us still do enjoy a scrap. Protecting us from each other, from harm and exploitation, is one of the oldest justifications for governance.

If you're a creator, someone whose imagination can bring joy and delight, you might be wondering where governments stand on one of the biggest issues of our times—the protection of creative works in the era of artificial intelligence.

The answer across the US, the UK and Europe, it would appear, is: Not on your side.

What's going on?

Let's start in the country that's had a profound influence on cultures around the world for over a century.

Underpinning America's creative genius and technological prowess are laws giving creators and inventors intellectual property protections through copyright and patents. This tradition has been built on creative industries forming a symbiotic relationship with tech.

Today that relationship has turned parasitic.

Silicon Valley, home to the most valuable businesses the world has ever known, is feeding off of creators by using their works to train AI models—without consent or compensation.

THE MAGA/TECH GIANT AXIS

The White House's recent AI Action Plan—a 28-page roadmap designed to preserve America's AI supremacy—avoided mentioning copyright.

Shortly after the Plan was unveiled, Donald Trump dropped a bombshell, telling a jubilant Washington audience of tech leaders and venture capitalists that America couldn't expect to maintain its AI lead over China if "every single article, book, or anything else that you've read or studied, you're supposed to pay for".

Trump's excuses for not paying could have been plucked from my newsletter's ever-popular AI-Copyright Deniers' Bingo Card.

Several publishers and creator groups are suing AI developers for copyright infringement. It's hard to escape the thought that Trump will somehow look to set aside those legal actions—anything to protect big, beautiful, American AI. Some media orgs have sought licensing deals with the hi-techs, but his comments on not having to reward creators will have undermined, if not killed stone dead, any nascent market for rights.

Trump is using the threat of increased trade tariffs to protect US national interests. So intense is the desire to see America win the race to an AI that's as smart as a human, that he's likely to take a harsh view on any nation seeking to impose regulations on Big Tech.

STARMER'S STALLING STRATEGY

Which brings us to the UK and a possible explanation for why the Keir Starmer government is so intent on kicking the AI and copyright can down the road for a few years.

More than 11,500 public responses were received to a consultation on whether UK copyright laws should be watered down to favor the interests of tech giants. Six months later, the country is still none the wiser about what those responses actually were and what ministers want to do.

The UK government could have added emergency protections to a data bill that would have let creators know if their works had been used to train generative models. But, no. After five consecutive defeats, ministers asked the UK's upper house to trust them, and the peers of the House of Lords reluctantly agreed.

The government is convening working groups on AI transparency and standards and has committed to a series of reports. You could be forgiven for thinking that it's a stalling tactic out of a scene from the British political satire Yes Minister. Why delay?

KISSING THE ORANGE RING?

Back to Trump. Britain has a trade deal with the US, but things could change at the drop of a MAGA hat should the UK go hard on creator protections. A similar situation exists in Europe where creators were given an opt-out in the EU's AI Act.

However, AI providers only need to reveal the top 10% of domain names that their crawlers have scraped. That, and the fact that they only need list domains rather than specific works, means the European Commission's transparency template is, as a creators' leader told me, "useless." Adding insult to injury: AI firms have two years to complete the template, and those who find it too much of a burden only need to state as much and walk away.

Why would Brussels go soft on Big AI? Once again, we're back to Trump. Both the UK and Europe appear petrified of doing anything that'll annoy the US hi-techs and incur Trump's wrath.

In January, Sir Paul McCartney called on the UK government to think again about its plans to overhaul copyright laws.

"We're the people, you're the government! You're supposed to protect us. That's your job," McCartney told the BBC, adding that ministers needed to "protect the creative thinkers, the creative artists, or you're not going to have them".

The silver lining in all this is neither will AI. Without the creators, there is no AI. Its models depend on a constantly updated supply of quality content. Something will eventually have to give. Just don't count on governments to step up.

Subscribe to Graham Lovelace's newsletter, Charting Gen AI for analysis and commentary on AI's impact on human-made media.



AI-COPYRIGHT DENIERS' BINGO

TRAINING AI MODELS ON COPYRIGHT PROTECTED CONTENT IS FAIR USE	IMPOSSIBLE TO TRAIN AI MODELS WITHOUT USING COPYRIGHTED DATA	ROBUST COPYRIGHT REGIMES HARM SMALLER AI START-UPS	TRAINING DATA IS PUBLICLY AVAILABLE	ALL CONTENT ON THE OPEN WEB IS FREWARE
AI TRAINING IS NO DIFFERENT TO HUMAN LEARNING	AI MODELS DON'T COPY ANYTHING	AI MODELS DON'T COMPETE WITH TRAINING DATA	COPYRIGHT PROTECTED CONTENT HAS NO ECONOMIC VALUE	COPYRIGHT HOLDS BACK PROGRESS
COPYRIGHT LAWS ARE MORE THAN 300 YEARS OLD	COPYRIGHT LAWS LACK CLARITY AND CERTAINTY		IT'S A MATTER OF NATIONAL SECURITY THAT WE DO THIS	PAYING CREATORS IS JUST TOO COMPLEX
MODELS DON'T REPRODUCE TRAINED CONTENT	AI MODELS MAKE SOMETHING NEW	COPYRIGHT IMPOSES A REGULATORY BARRIER	WE NEED TO MAINTAIN OUR AI SUPREMACY OVER CHINA	CHINA DOESN'T CARE, WHY SHOULD WE?
COPYRIGHT EXCEPTIONS ARE KEY TO ATTRACTING AI INVESTMENT	COPYRIGHT LAWSUITS COULD BANKRUPT AI COMPANIES	JAPAN AND SINGAPORE ALLOW FREE SCRAPING	WE'RE LOWERING BARRIERS TO CREATIVITY	CREATORS OVER-ESTIMATE THE VALUE OF THEIR WORKS IN TRAINING AI MODELS

GRAHAM LOVELACE BEGAN COLLECTING THE AI INDUSTRY'S EXCUSES ABOUT WHY, DESPITE ACCESS TO "GOD-LIKE" TECHNOLOGY, IT COULDN'T OBEY COPYRIGHT LAW. THE RESULT IS THE AI-COPYRIGHT DENIERS' BINGO CARD. PLAY ALONG AT HOME!

DOWNLOAD THE CARD, WITH THE TRUTH BEHIND THE EXCUSES, AT "CHARTING GEN AI".

BUILDING AN ARTIST FRIENDLY

AI

By Tommy Flanagan, Editor, Faultline

Incantor is positioning itself at the intersection of intellectual property protection, generative AI, and content creation

"Current AI tools are flagrantly contemptuous," begrudged Incantor CEO Lauren Oliver.

With many mainstream GenAI platforms, from OpenAI, Google, to DeepSeek, facing

backlash for scraping copyrighted material from the web, Incantor claims to have built a proprietary "Light Fractal Model" trained only on licensed data, with built-in attribution tracking.

Their idea is to cultivate a creative marketplace, where every media asset that is contributed (voice, image, script, and eventually video) will be tracked, credited, and compensated by a 10% share of any resulting revenue streams.

Incorporated in January 2025, the eight-person Incantor is about as raw as start-ups come. The AI model, sparked by Oliver's own literary PTSD as a best-selling American novelist, has the potential to be successfully disruptive.

But to reach that stage however requires scale, accompanied by a steady dose of "duct tape and wishes", which is essential to get 50% of US technology start-ups to survive to their fifth birthday.

Oliver claims, with a grin, that Incantor is already at a stage where it is needing to scale, which could present teething problems for such a nascent operation, forced to run before it can walk. However, the rise of lawsuits between Hollywood writers and Gen AI giants, described as an apocalyptic threat to creative livelihoods, is all the justification needed for bootstrapping Incantor at personal expense.

TURNING WORDS INTO ACTION

Currently, Incantor is a text in-voice out model. We are shown a quick demo of a synthetic voice based on a real actor's IP. The text-to-voice model plays the statement "Oh, my God. What do you mean she's dead?" The output can be pulled around a wheel to convey 16 different emotions (and growing). The result is an impressively expressive range from just two data sources.

This immediately reminded us of the NotebookLM experiment we ran with the Faultline podcast last year in which we generated two AI personas to discuss one of our articles. Let's just say it didn't catch on, and it was comically cheesy in parts. But our AI podcasting experiments are music to the ears of Incantor with the company planning for an automated pipeline to transform media into adaptive podcasts.

Oliver is optimistic that Incantor's proprietary AI-generated outputs, including a couple of trialed podcasts, are a cut above what typical

the typical transformer/diffusion models available can produce.

KEEPING HOLD OF ATTRIBUTION

Incantor has partnered with an unnamed animation studio to train a lightweight AI model that can animate characters without relying on traditional rigging. The model was trained directly on performance data, allowing it to generate animations autonomously, with only a day's worth of manual refinement needed in the animation pipeline.

A separate AI-driven lip manipulation demo was also teased, but unfortunately an NDA blocks us from opening that door, for now.

Where Incantor could fall over is if the attribution model fails. If content IP is leaked outside of the platform and manipulated, then there is no way to prove the provenance and therefore protection of the owned IP.

This is why Incantor is likely to follow more of a metadata-based model similar to that of C2PA, which works fine in controlled environments, such as a TV studio or a trusted newswire, where media passes through known systems. But once that content enters the open internet, that metadata can become a liability. If your authenticity model collapses the second someone re-uploads a file, then your entire backbone falls apart. ➡

Statistical Analysis vs. Fractal Mathematics

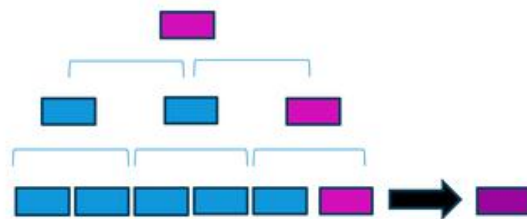
Statistical Analysis:

Remembering long chains of tokens to accurately predict next token

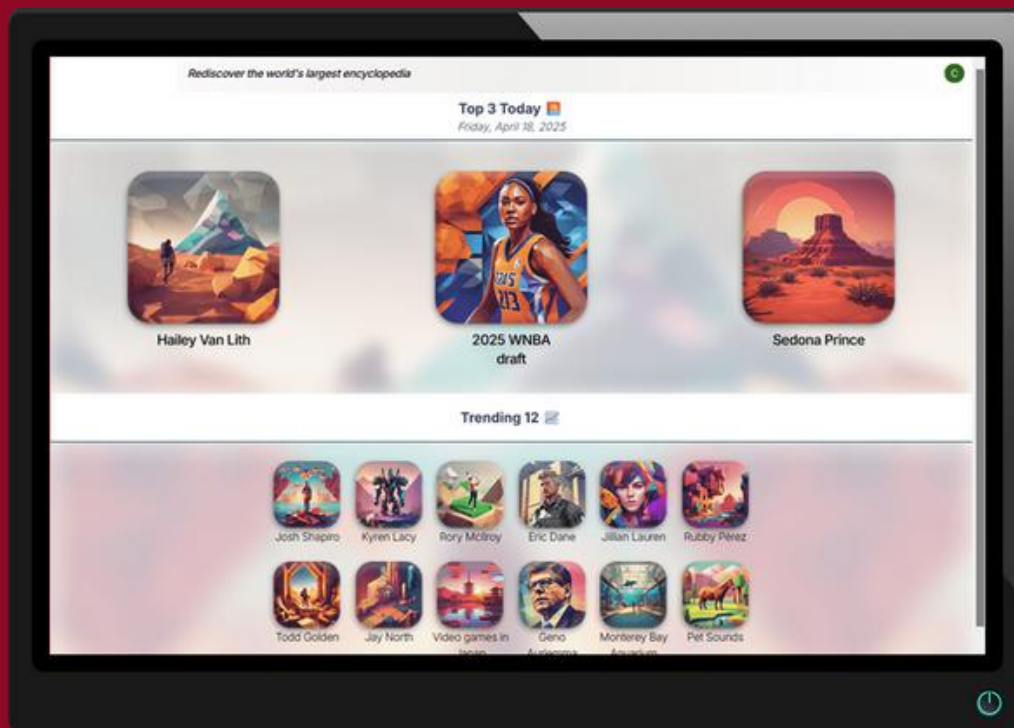


Fractal Mathematics:

Compressing higher-dimensions of contextual similarity for better and faster predictions



Incantor uses a more efficient model than the statistical guessing game used by most Gen AI



Oliver notes that Incantor is exploring tokenizing attribution, though she dismisses going down the blockchain route—bemoaning the distributed ledger approach for not scaling. This contrasts with claims from blockchain advocates that the technology will scale once (if) the decentralized web 3.0 revolution takes off, abandoning the centralized internet standards bodies imagine.

A LESS RAVENOUS AI?

Returning to the Light Fractal Model itself, these algorithms, based on fractal mathematics—geometric shapes that form infinite patterns that could be compared to neural activity in the human brain—aim to reduce data usage by between 10x and 100x.

That in turn delivers power consumption reductions orders of magnitude below what traditional incumbent AI companies are generating, while at the same time claiming to achieve performance orders of magnitude over what these LLMs are outputting.

Oliver did not have any energy benchmarks to hand, but we have been promised a follow-up with hard supporting data.

If Incantor can live up to promises of beating the big boys over quality, price, and power consumption, while maintaining attribution

and ownership of IP with royalties to boot, then we are on to a winner.

Does it sound too good to be true? Possibly. But that is primarily because the company cannot publicly share a customer case study.

To grasp the SaaS-based model of the creative-driven marketplace, Incantor provided the following example:

“Let’s say John and Jane Doe have contributed voice timbers to create a Synthetic Voice #1. That Voice is then used by one of our partners to serve as narrator for one of our channels, which begins to earn ad revenue in its second year. We will create a pool of contributing sources, and their relative contributions to the finished IP, in which John and Jane Doe will be represented.

“When we begin earning Revenue, they begin earning royalties. Additionally, their contributions will be credited at the end of every piece of media that uses their data.”

Once Incantor achieves the scale that its business model relies on—with a larger pool of contributing source IP creating a higher chance of generating royalty-earning revenues—then we will reassess whether it really could be a hope for rejuvenating the AI-scorched landscape of IP ownership. 🟡



Faultline

If this article made you think, wait 'til you see the content we don't share

Faultline is the must-read weekly briefing for people who build, invest in, or disrupt the video delivery chain—from streaming giants to disruptive start-ups.

We pride ourselves on a policy of zero press release parroting. We cut through the corporate fluff to deliver readers sharp, skeptical, and sometimes uncomfortable truths about where the media & entertainment industry is headed next.

**Don't take our word
for it. Here's what
subscribers say:**

"We use Faultline to inform, and occasionally challenge, our view of the competitive landscape. The qualitative analysis, which sticks closely to an investigative-journalism model, allows us to separate fact from fiction, and to probe the chasm that can exist between what competitors claim to do, and what they actually deliver into the hands of customers."

"Faultline provides our strategy team with deep, accurate and timely knowledge. It is this unfiltered and objective data, written in human readable language, that ensures our fast continued innovation and market response."

"I don't know how the rest and their meagre publications survive by just passing through the press releases."

Want more?



Subscribe now at www.rethinkresearch.biz/faultline



Or scan the QR code



Published by **Rethink Technology Research**

20+ years of insider analysis on the economics of disruption in video, wireless, energy, and automation

NEXT ISSUE

Winter 2025

CONTENT SOVEREIGNTY

Time to take back your
creative kingdom

also

**Better climate
storytelling**

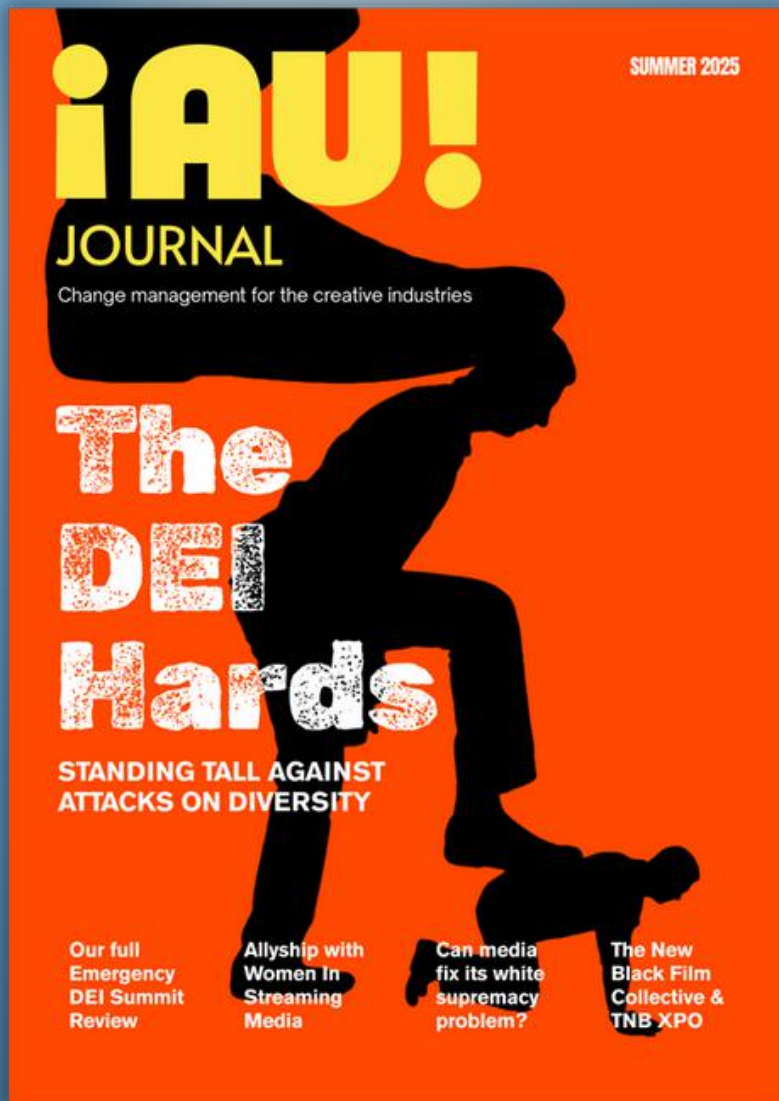
**Line producing
in hard times**

Monster Lab



**WE HOPE YOU'VE ENJOYED
ISSUE TWO OF ¡AU! JOURNAL!**

**CLICK ANYWHERE BELOW
TO START READING ISSUE ONE!**



**AND CLICK HERE TO GET
THE ¡AU! NEWSLETTER**



