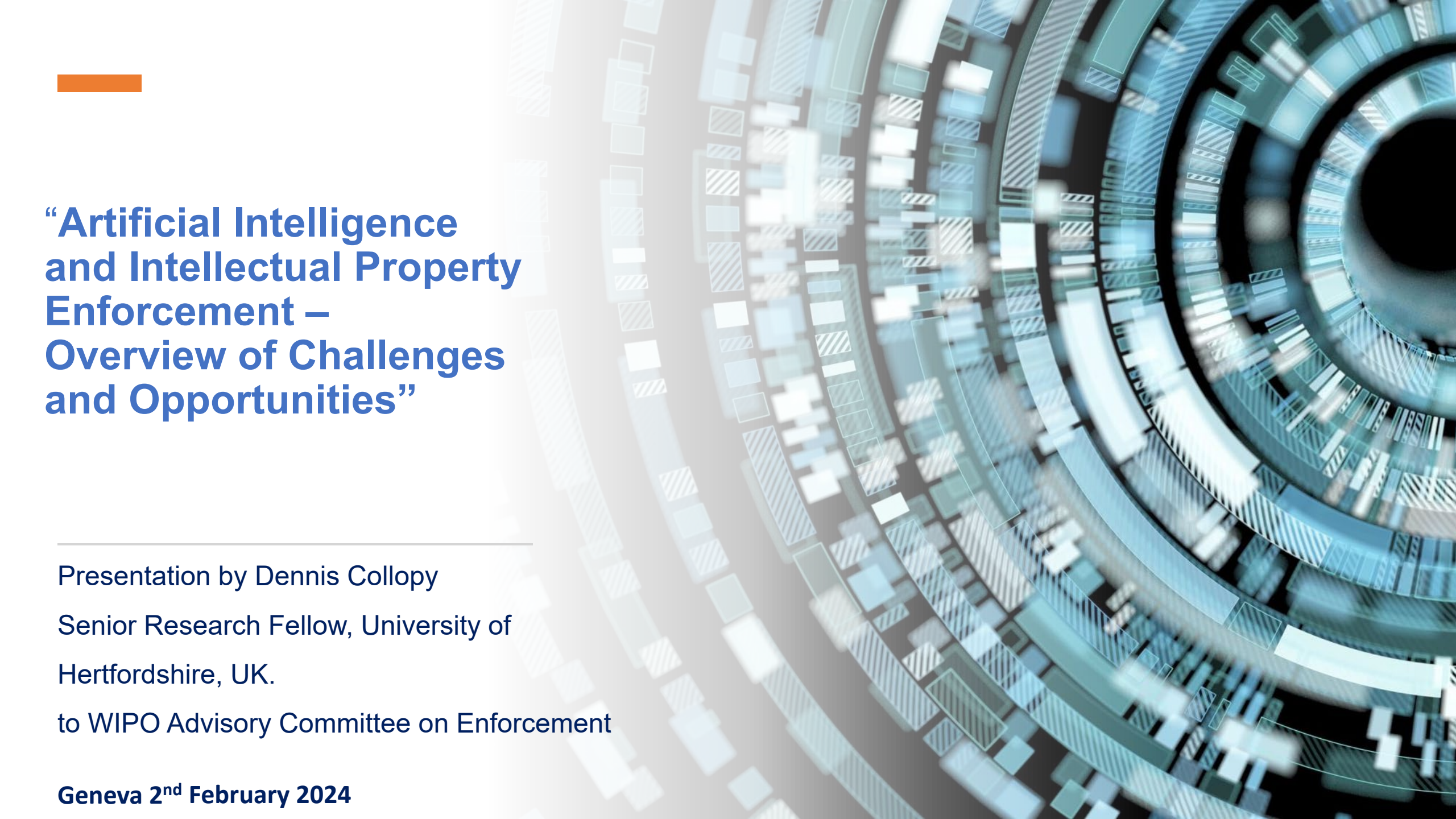
“Artificial Intelligence and Intellectual Property Enforcement – Overview of Challenges and Opportunities”

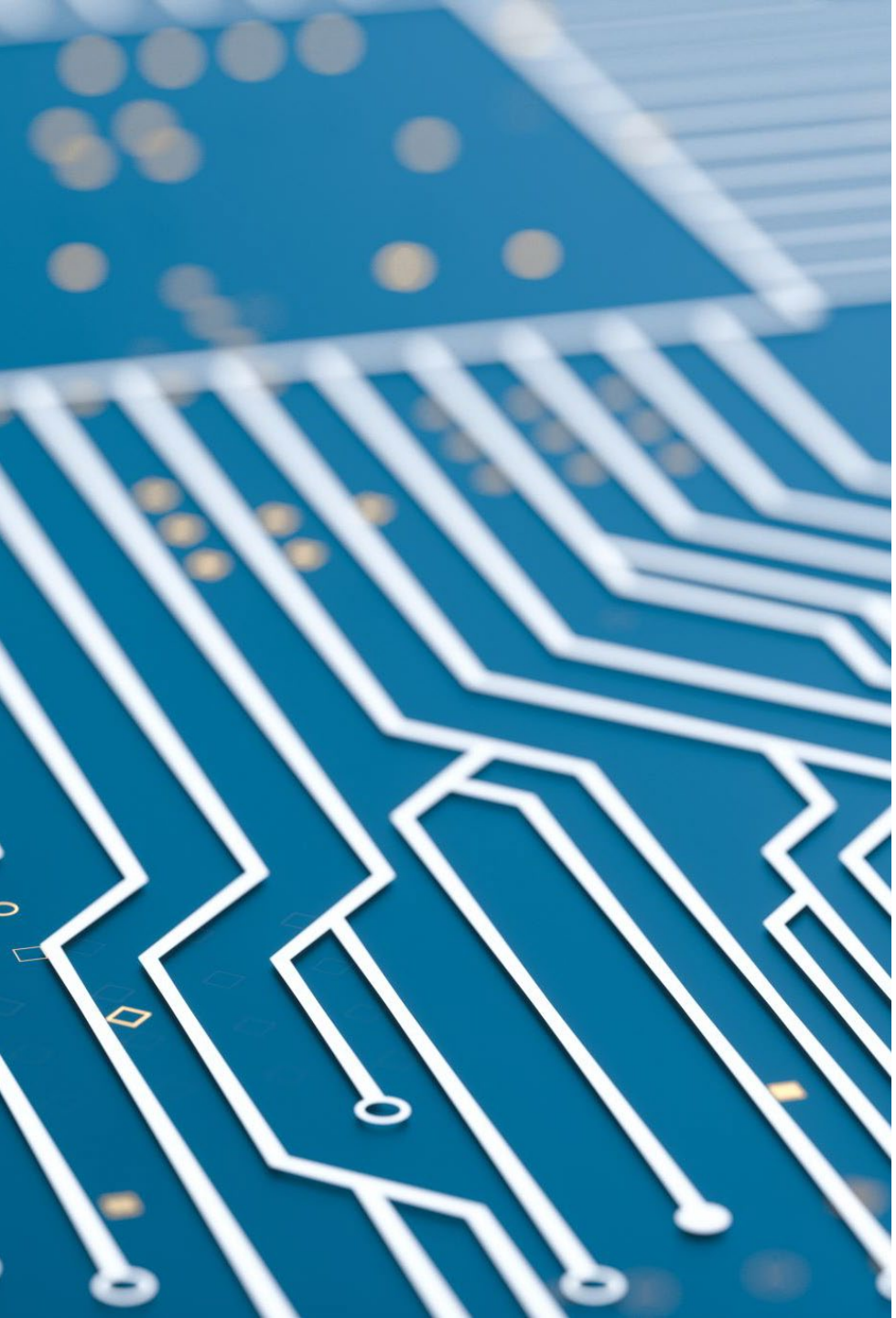
Presentation by Dennis Collopy

Senior Research Fellow, University of Hertfordshire, UK.

to WIPO Advisory Committee on Enforcement

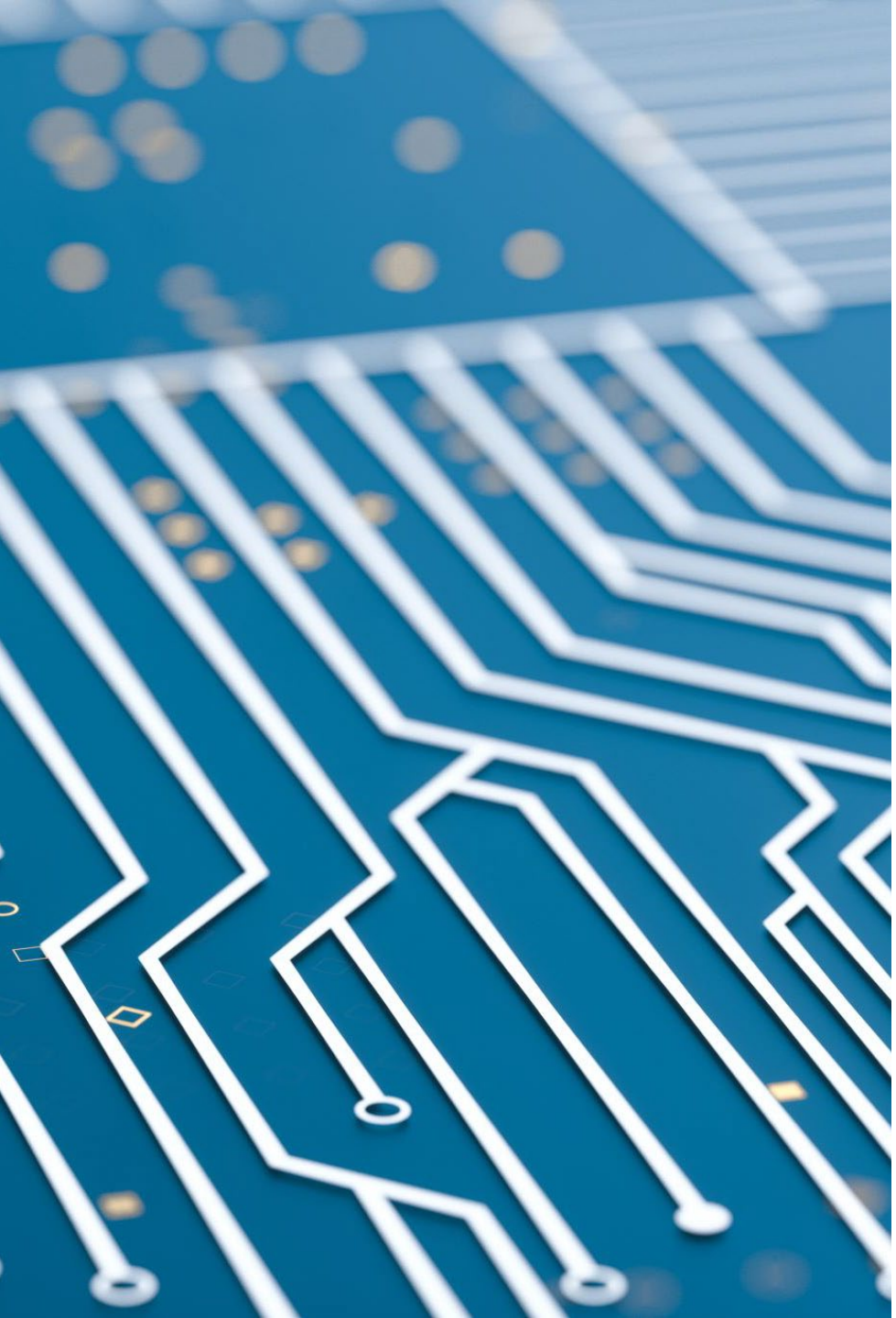
Geneva 2nd February 2024





Objectives and Aims

This contribution is based on the research study *Artificial Intelligence and Intellectual Property Rights Enforcement*, which was commissioned by the Intellectual Property Office of the United Kingdom in 2021 to evaluate whether and how artificial intelligence (AI) can be used to track and trace intellectual property right (IPR) infringing goods, as well as to assess the potential use of AI by those infringing IPR.

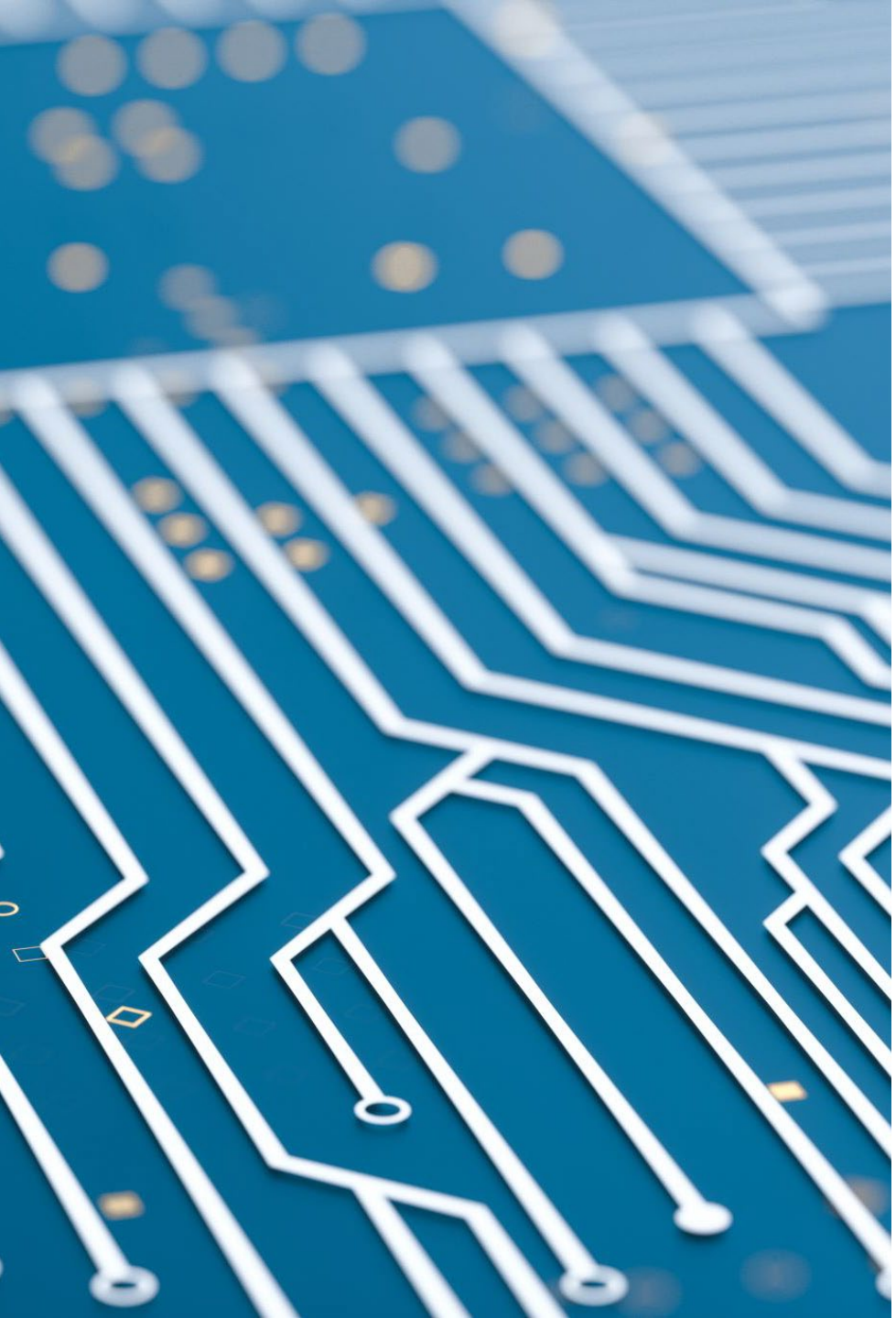


Objectives and Aims (cont.)

The project aim was to review and collate existing literature and to capture the views of those with expertise and experience on the existing IPR enforcement landscape as to:

- how AI is currently used by right holders to protect and enforce IPR and
- assess threats from those infringing IPR.

The research covered five IPRs: patents, trademarks, designs, copyright and, notably, trade secrets.



Methodology

The project involved a two-phase process including:

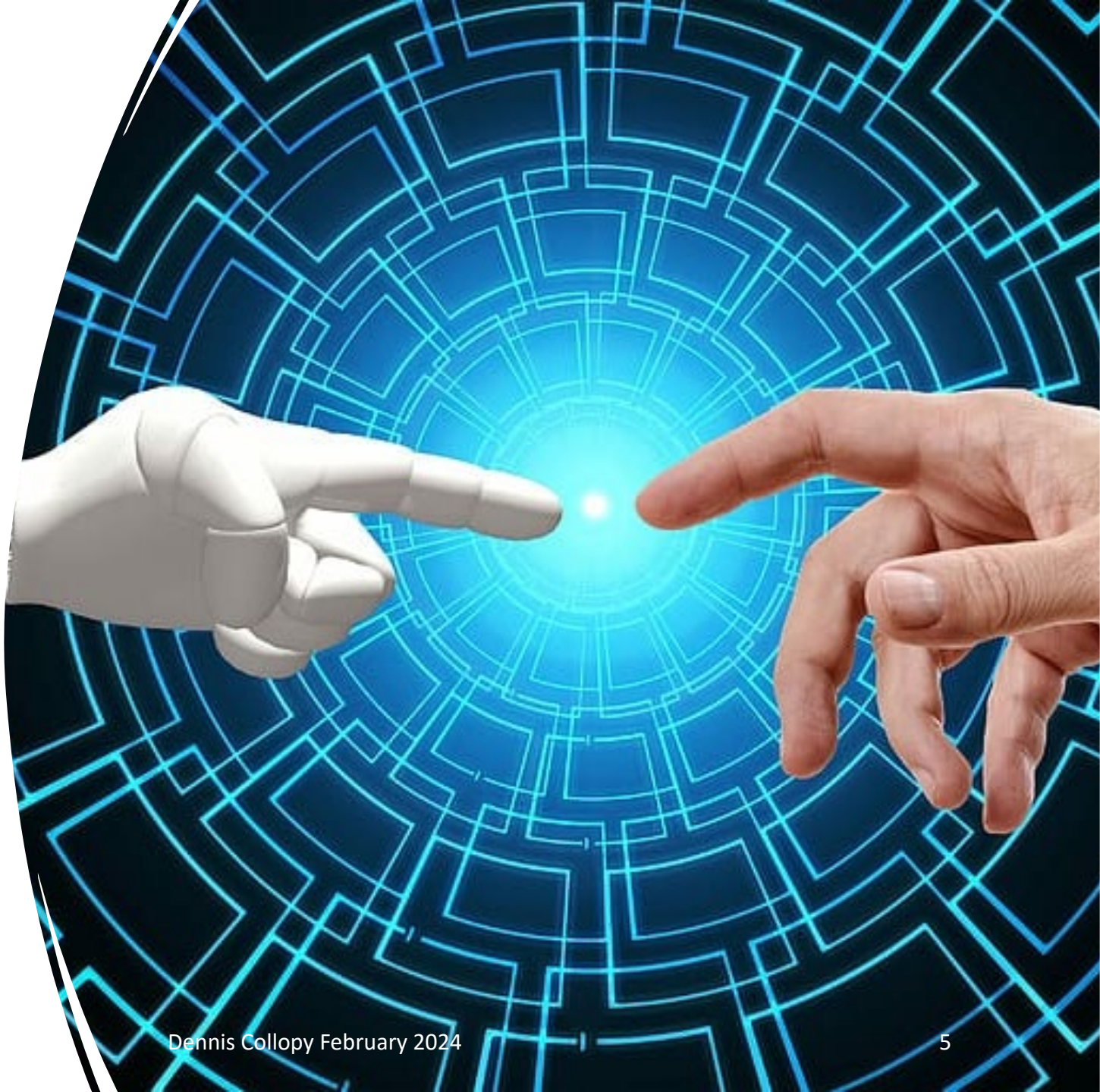
1. A critical examination of the AI and IP enforcement literature relevant to the five IPR under consideration, produced by government, academia and industry to identify core themes and outcomes

2. This literature review allowed for the creation of a questionnaire as the basis for an extensive range of interviews with relevant stakeholders across industry, enforcement agencies, academia, legal practitioners and the judiciary to capture fresh and current insights of the current issues.

Definitions

At the outset, it was important to carefully define the terminology used, given the proliferation of definitions for AI.

The clearest and most succinct definition of AI as "***human intelligence exhibited by machines***", was provided by one of the co-authors of the UKIPO study and AI expert Professor Kevin Curran.

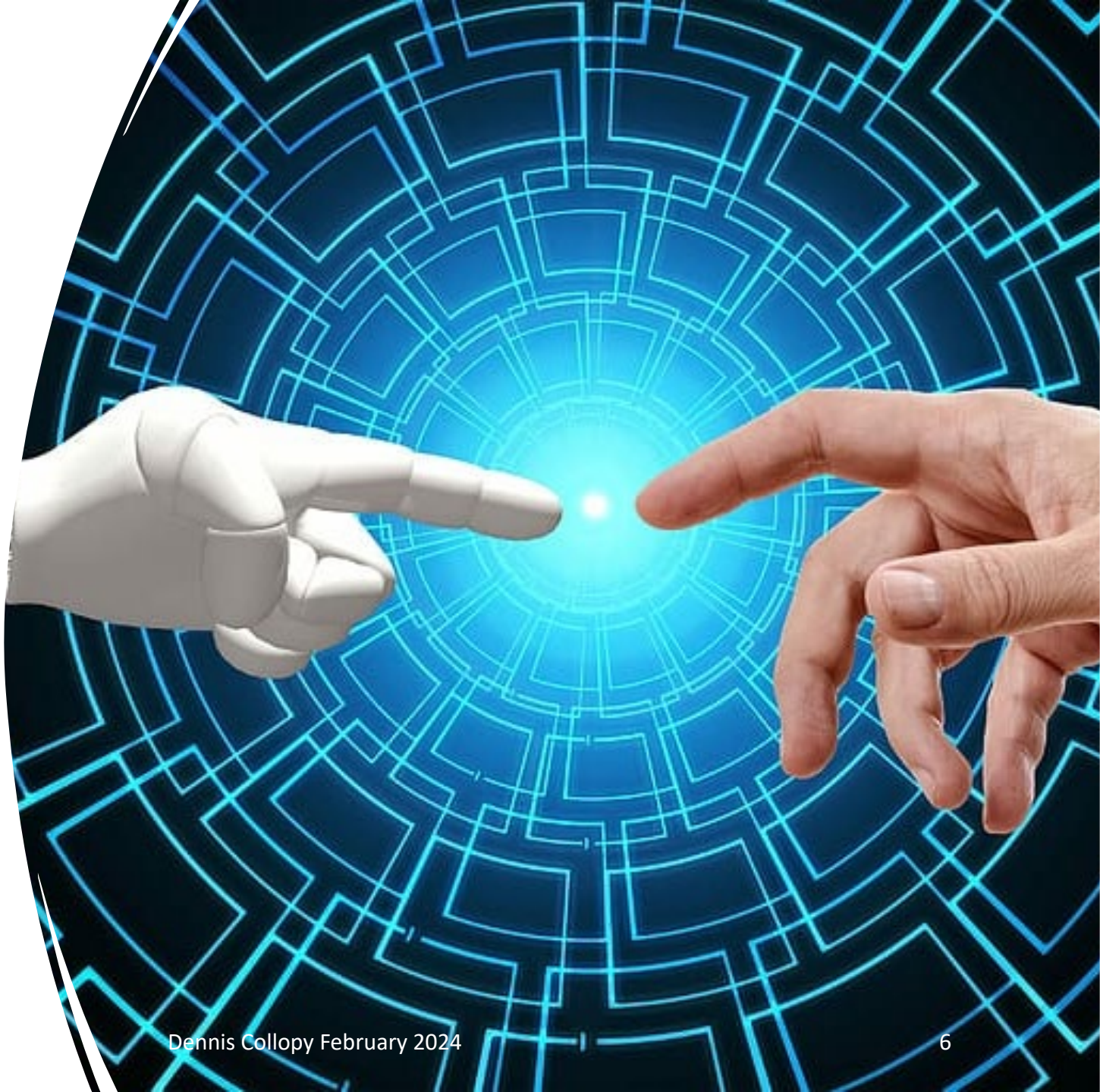


Definitions (cont.)

Our research focused on the subset of AI, known as narrow AI, in the form of machine learning (ML).

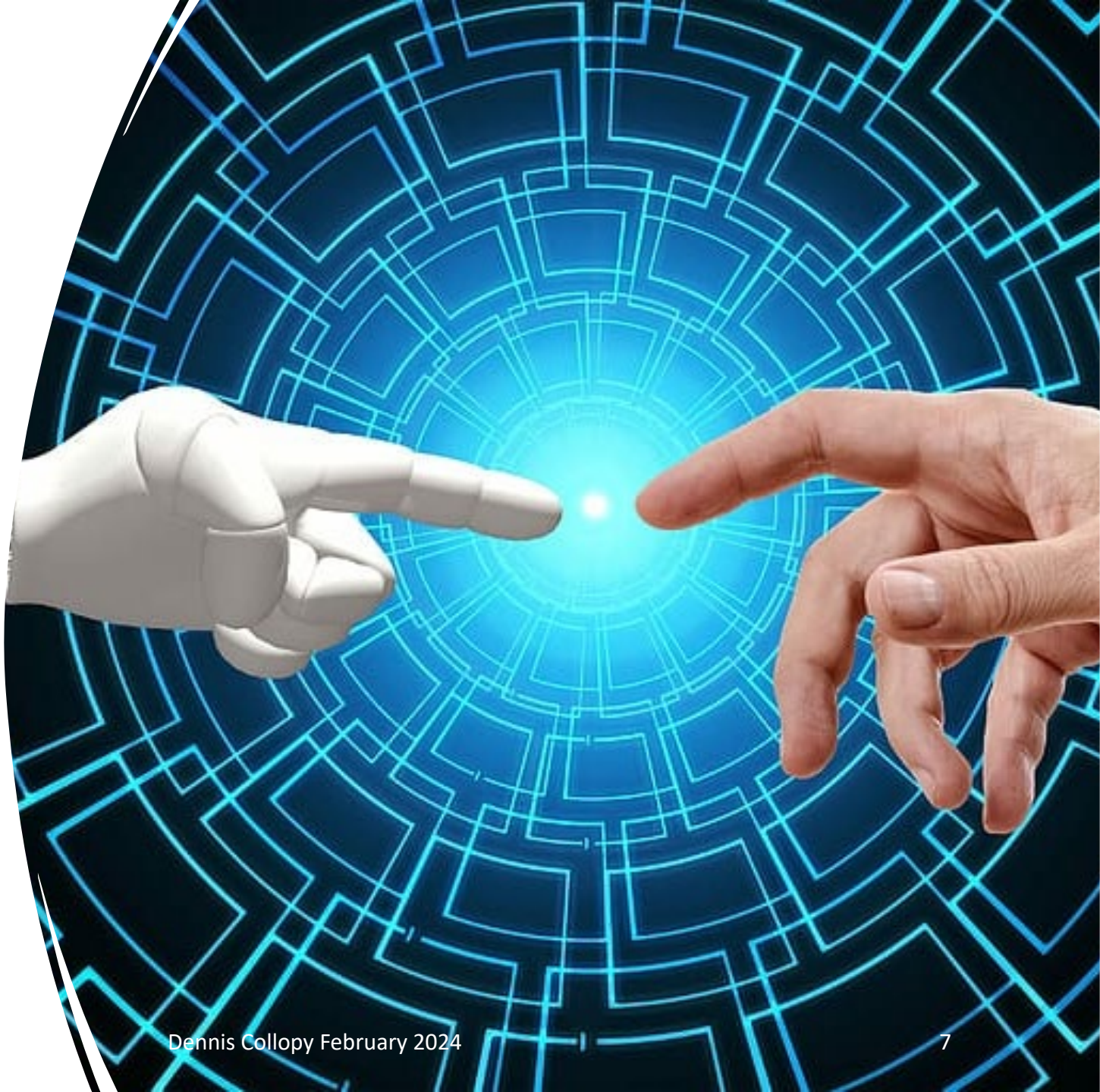
ML enables the creation of systems "***that can learn from experience to find patterns in a set of data***" and thus are able to infer or predict an outcome.

These processes involve a few challenges as well as opportunities that were the focus of our original study.

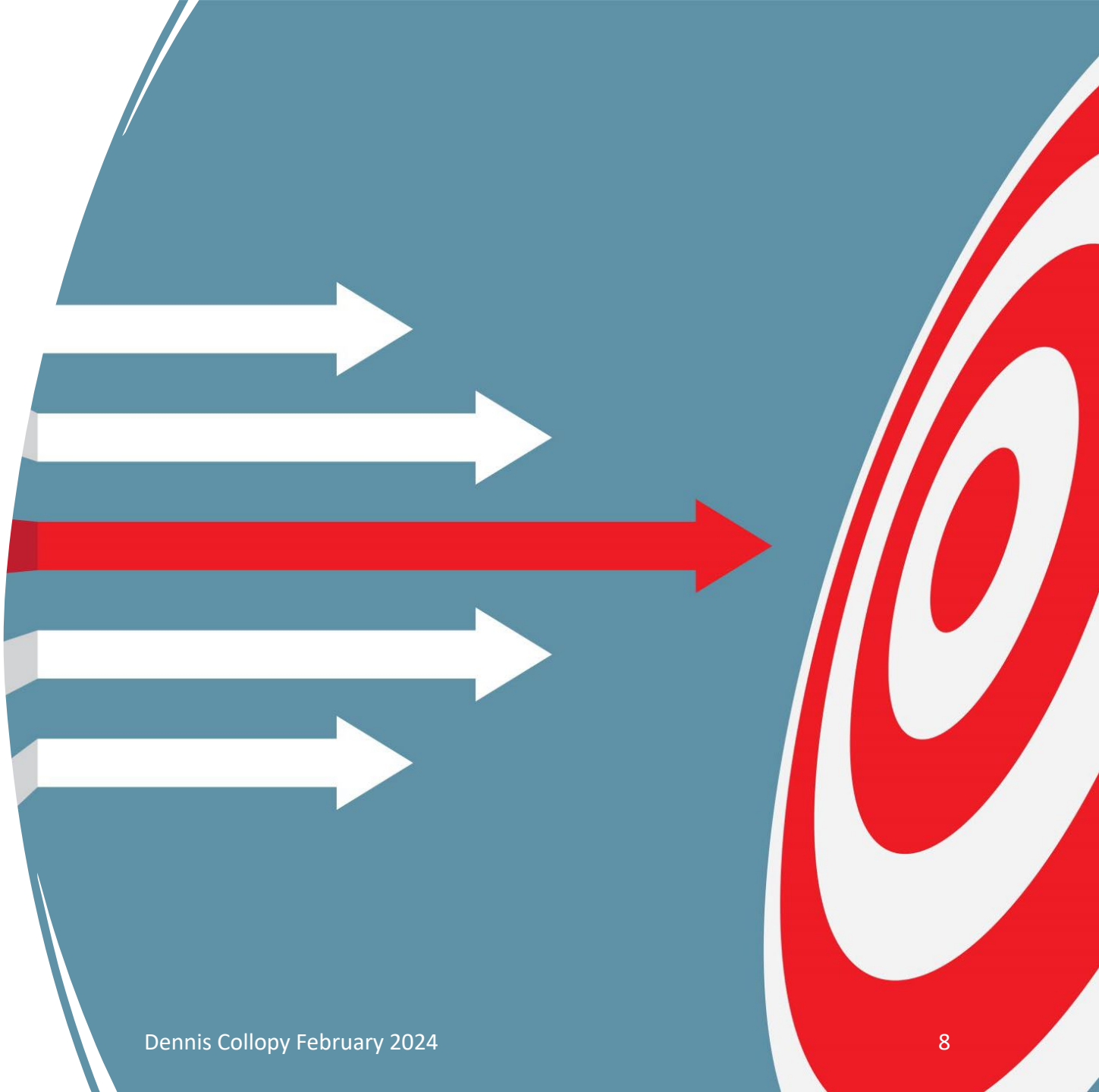


Definitions (cont. 2)

- Narrow AI is the only form of AI that exists today and is trained to perform a single task, and unlike general AI, cannot operate outside of that defined task
- Any other form of AI is still “theoretical”
- OpenAI’s ChatGPT is a form of Narrow AI
- Non-transparent AI (also known as black box AI) cannot be inspected in the same way as systems with a full audit trail.



Research Findings: Main Opportunities for AI



Opportunities 1

Copyright

There is an opportunity for increased use of AI tools in copyright enforcement, especially given certain apparently successful automated anti-piracy systems.

As a filtering tool, AI helps to identify infringing content and reduce human workloads, but it needs accurate and adequate training data. YouTube's Content ID is an example of an apparently successful AI tool.

Research has shown Content ID to work 'relatively well' in removing apparent infringing content from YouTube, but critics claim it is not 100% successful

Opportunities 2

Designs

Improved image recognition capabilities could help identify potential infringements.

The UK's s **Anti-Copying In Design** (ACID) maintains a databank of over 300,000 designs (including unregistered designs) that could provide data to train an AI to recognise infringing designs

Opportunities 3

Trademarks

AI tools could help trademark enforcement analysts, if trained on very large datasets, freeing up human resources.

There is scope for further development of enforcement solutions in close cooperation with consumer-facing online platforms that deploy AI tools for monitoring content.

The new range of tools provided by the European Union Intellectual Property Office (EUIPO) offer track-and-trace solutions, risk analysis systems and use of AI/ML in detecting suspicious and potentially abusive domain name registrations.

AI could play a part in enforcing rights implicated in different types of cybercrime and in detecting counterfeits as an aid to human actors.

Opportunities 4

Trade secrets

Trade secrets, especially for AI-related inventions, need enhanced protection against misappropriation.

Security measures such as AI-based techniques, including neural encryption techniques, may offer greater protection.

Opportunities

Summary

Detection of copyright infringements is the most common example of AI use in IPR enforcement at scale, provided robust training datasets are available.

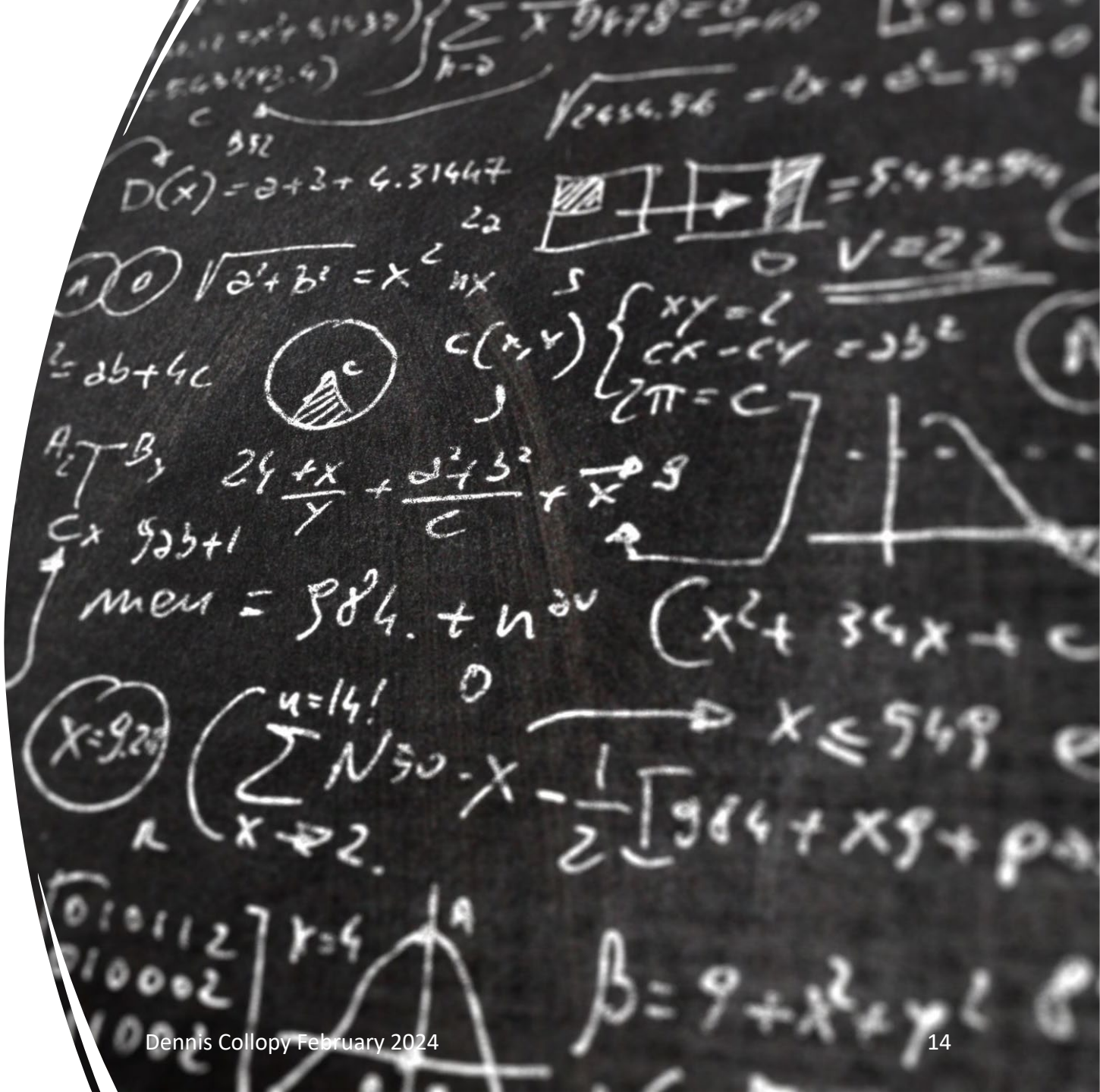
If implemented similarly, AI could be also used to identify infringements of designs and trademarks, thereby reducing human resources.

Intellectual property analytics could improve the discovery of relationships, trends, and patterns of IPR infringement for improved enforcement decision making.

AI can only improve and become more accurate and faster, detecting patterns in a far superior manner to humans.

Overall, AI is a useful filtering tool and an aid to human analysis in speeding up the processes of identifying infringing content.

Research Findings Challenges in using AI



Challenges 1 Copyright

- There are concerns about the costs and resources involved in using automated tools for enforcement against copyright infringements.

- Such tools may be beyond the means of many SME right holders, who will tend to rely on CMO's and trade bodies to enforce their rights.

- Automated anti-piracy systems are opaque and reliant on hard-coded automated rules using dynamic, potentially unpredictable, and non-transparent algorithms for decision making.

Challenges 2 Designs

- AI tools could help interrogate registered design databases. However, AI may not help identify infringements of unregistered designs or those reliant on copyright.

- Apart from existing databases, such as the one maintained by ACID, the costs involved in using AI to identify infringements benefits large firms owning portfolios of designs.

- The enforcement of registered and unregistered designs must consider the use of computer-aided design (CAD) and AI-generated designs, especially where unregistered design rights are used to train Ais.

Challenges 3 Trademarks

- Trademark enforcement is hampered by data-sharing issues between industry, government and enforcement agencies that inhibit the use of automated tools at scale.

- Enforcement groups struggle to extract clean data from infringing websites and collate effective large data samples for the training of AI.

Challenges 4 Patents

- AI use in enforcing patent rights needs to combine a blend of human and technological knowledge.
- The complexity of language involved in the application for patents as well as the complexity, cost and effort of taking legal action are challenges to enforcement.
- In addition, restrictions on using evidence of reverse engineering in English court proceedings make infringement of certain patent rights difficult to prove.
- AI-generated or AI-assisted IP infringements must relate to the actions of a legal ‘person’, and, as such, enforcement may need to be taken against those operating the AI.
- Enforcement against infringement of patents relating to AI may be hindered due to uncertainties associated with ‘black box’ AIs that defy human comprehension.
- AI tools are perceived as insufficiently nuanced or adapted for patent law, which requires lateral thinking and interpretation.

Challenges 5 Trade Secrets

- Trade secrets enforcement is impaired by the perceived risk of public disclosure during court proceedings, and therefore infringement issues are commonly settled out of court. Enforcement of trade secrets is also impaired by uncertainty around what may legally constitute a trade secret.

- AI is seen as one of relevant factors involved in the increase of cyber thefts of trade secrets, which in turn requires new AI and ML tools to combat the cyber-attacks.

- There is also concern that AI could be misused to hack into and get hold of trade secrets as opposed to protecting them.

- Trade secrets cover commercially valuable information not protected by patents or other IPRs, but enforcement depends on taking reasonable measures to keep such information secret as they are only useful for as long as they can be kept secret.

- In this regard, AI is seen as less immediately useful, given the nuances and variety within trade secrets and the fact that they are not intended to be public facing in the first place.

Challenges 6 Ethical issues

- The ethical limitations of using AI in IPR enforcement include the quality of (such as inadequate or incomplete) training data sets involved in the decision-making processes, as well as systematic and inherent human bias that could lead to unfair or incorrect decisions.

- There are also currently imperfections in the technology itself, including the lack of transparency (especially as regards “black box AI”) and accountability as well as an incomplete knowledge of how the AI’s work.

- There are also fears over the inflexible decision-making process involved with an AI that could lead to ‘over-zealous blocking’ of legal content.

Challenges 7 Legal issues

- AI tools would need retraining to meet the needs of different IPR laws in different territories.
- There is also the fundamental challenge of maintaining GDPR compliance when AI training data involves using mass volumes of personal or sensitive data.
- There is a danger of “bad actors” harnessing AI, such as the ability to re-upload content after it has been removed by takedown notices.

Challenges Summary

- The main challenges are the quality and quantity of training data needed for the effective use of AI in IP enforcement, as well as the crucial ethical and moral issues involved.
- An AI system is a resource-hungry process, and there is a clear link between the volume of data used by the AI and the accuracy of the results.
- The volume, quality and currency of training data are a common concern. Training AI tools is time-consuming and requires constant updating.
- Given the current limitations of AI as well as the ethical concerns, AI should currently only be an initial tool for flagging content to a human analyst for verification, rather than for enforcing IPR independently.

Conclusions and recommendations

Conclusions 1

Overall, the number of challenges identified exceeded the number of opportunities.

This was mainly a result of the number of fundamental issues relating to AI in the enforcement of Patents and Trade Secrets.

There remain other concerns about the use of AI in IPR enforcement, and these include several relevant case studies.

Conclusions 2

Warnings around the common methodological issues relating to the use of ML in the quantitative sciences were highlighted in a 2022 Princeton study;

The UK's long-running Post Office Horizon software scandal highlighted "*the dangers of humans blindly accepting the output of automated systems as reliable evidence*".

Similar issues could occur in other organizations that have reduced technology resources, outsourced critical expertise, and adopted less suitable auditing processes.

Conclusions 3

The Australian government's failed experiment with Robodebt, which the ACS described as an "AI Ethics Disaster".

The emergence of adversarial ML, where bad actors can exploit vulnerabilities to exploit AI systems and alter their behaviour to serve a malicious end goal. These attacks can involve poisoning (of the training data) or evasion attacks, many of which go unnoticed until there is a ML critical failure.

Recommendations

We remain confident of the ability of AI /ML to offer scalable solutions to assist the enforcement of some, if not all IPRs under consideration. We also stress that AI/ML itself is constantly improving.

But we cannot recommend the increased adoption of the technology without emphasizing the significant caveats described earlier.

We recommend careful piloting of any new AI-based IPR enforcement system to determine whether the system design takes account of the above drawbacks.

QUESTIONS

countercheck

Global Standard Anti-Counterfeiting Software

Connecting brands with logistics firms.
Helping law enforcement authorities.

Problem

PROBLEM

Logistics firms are transporting an increasing amount of illegal products

Global scale

OECD reports a **€420 Billion problem**, 3.3% of global trade.

Volume

EU alone deals with **25** Million **counterfeit parcels monthly.**

Customer spend

Logistics firms **involuntarily harm** their partners.

E-commerce

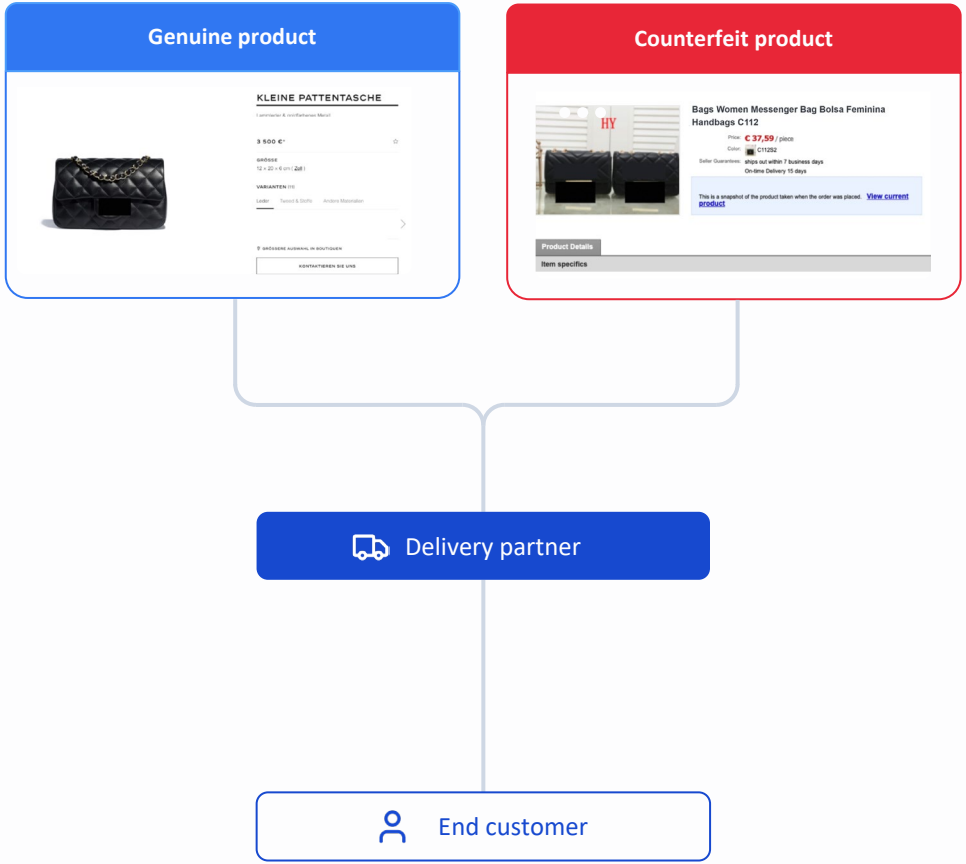
Counterfeiters leverage e-commerce for **direct consumer access.**

Delivery

Small parcel delivery enables **quick and cheap counterfeit distribution.**

PROBLEM

Disrupting counterfeits supply chain might be challenging



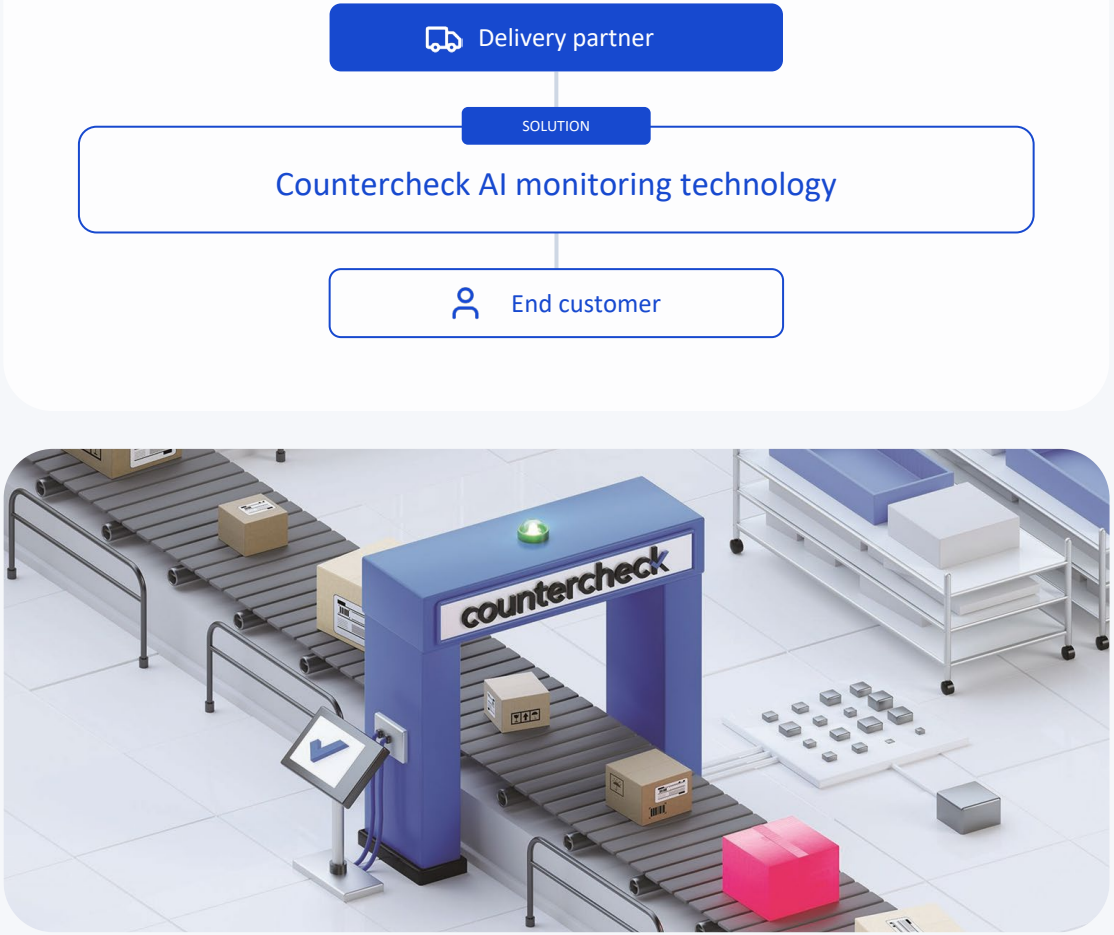
Solution

SOLUTION

AI-powered monitoring technology

Founded in 2021, Countercheck is the global standard anti-counterfeiting software for logistics firms.

The only way to scale the removal of parcels containing counterfeit goods is to **introduce a global layer of software that monitors all parcels worldwide.**



SOLUTION

Backed by BEUMERGROUP

Empowered by Beumer Group's expertise, we are able to seamlessly install our software in any sortation center, working with both Beumer and other hardware, to intercept parcels containing counterfeit and illicit goods.

“

Countercheck is a game changer in the fight against counterfeiting.

Dr. Christoph Beumer
CEO, BEUMER Group

Existing hardware

+

Countercheck software

=

Blocking counterfeits

Technology

SOLUTION

Ultimate technology

We establish a risk profile for each parcel coming through the sortation belt in just 0.6 seconds. If the risk profile is more than 75%, we sideload the parcel.

Image Processing

We handle camera images entirely on-site, with no reliance on external API calls. All processing is done locally, ensuring efficient and secure operations within our premises.

Optical Character Recognition - OCR

Our market leading reading models effortlessly interpret a wide range of shipping labels, showcasing versatility and solidifying our position in the industry.

Machine Learning

With precision and accuracy, our algorithms excel in detecting and responding to given specifications, providing a robust solution for targeted identification and analysis.

https://youtu.be/-EUEp_LS194

Geographical presence

HUBS

Geographical presence

With installations in United Kingdom, Netherlands, Norway, France and more by the end of the year, Countercheck is on it’s way to become the Standard Software to detect counterfeit and illicit parcels.

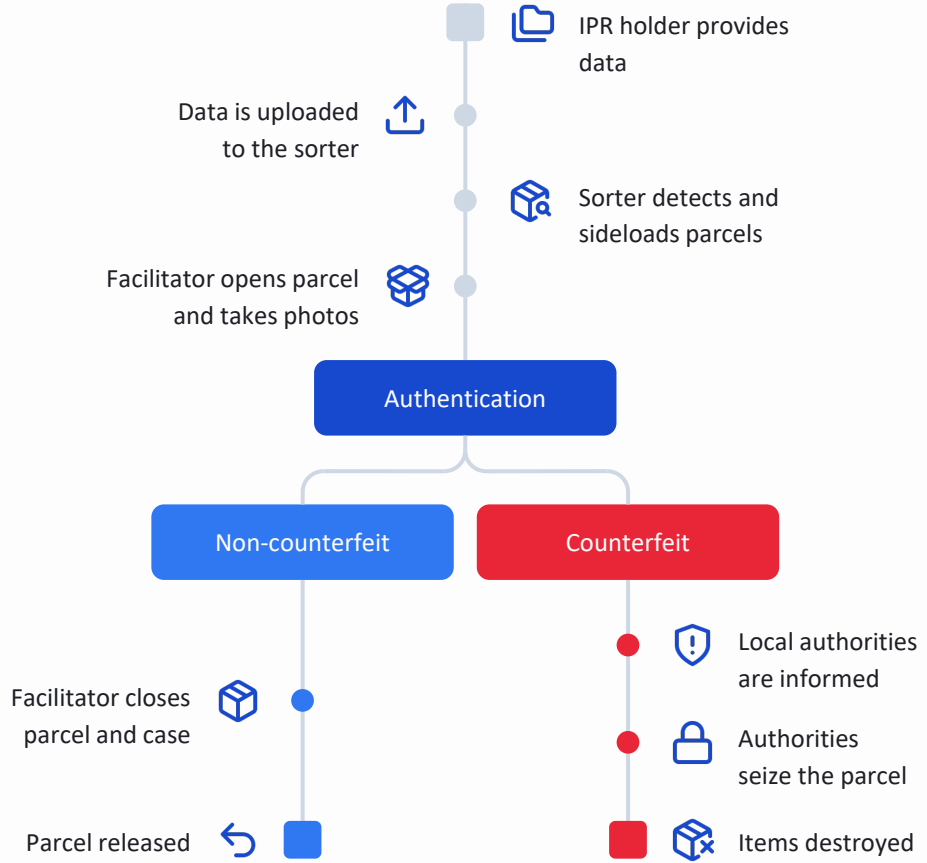
60 million
Parcel cleared/month

100 milion
Parcel cleared/month by Q2 2024

Process as designed by Countercheck

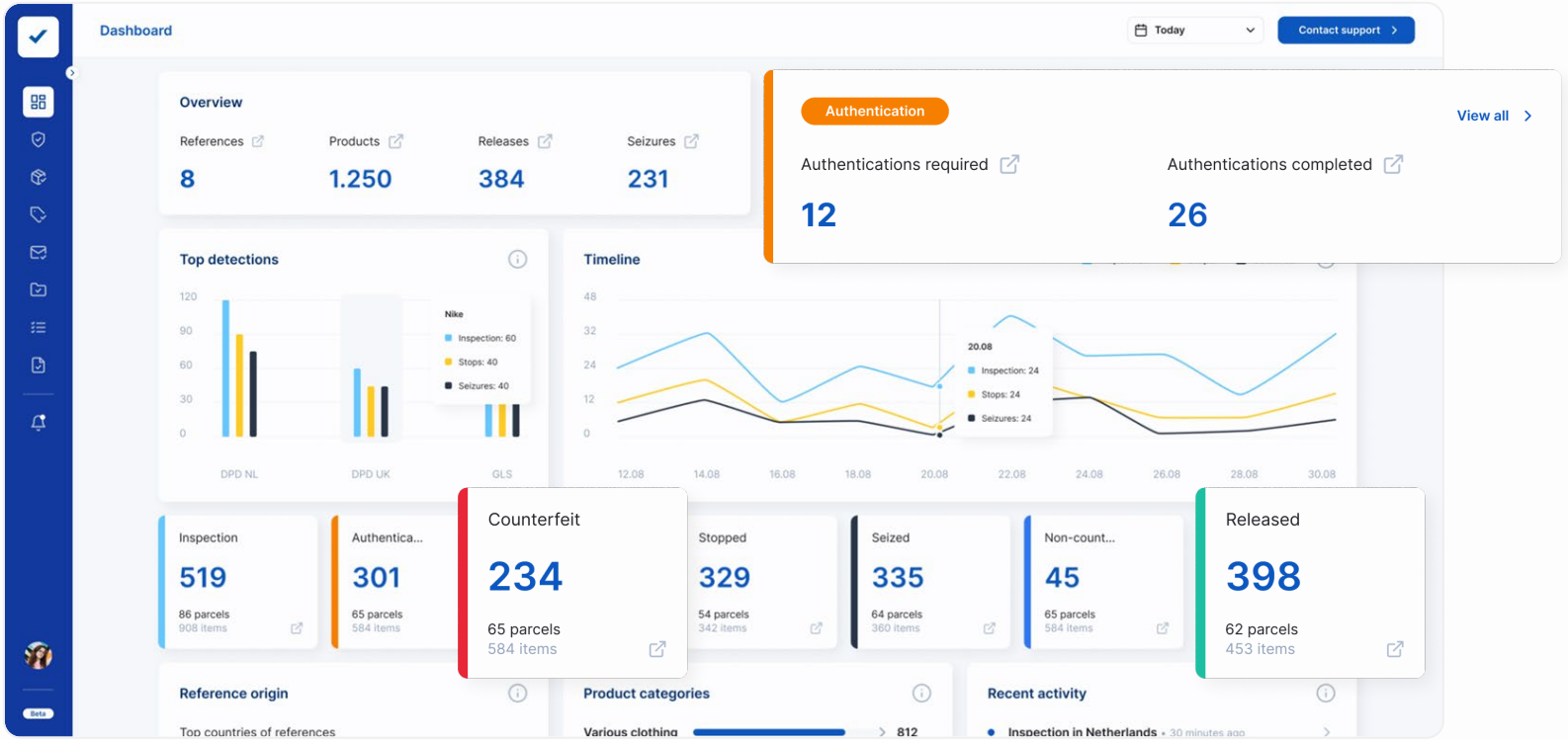
PROCESS

From catching to destruction



Platform

Total control over counterfeit goods with our platform



Statistics

HUBS

Key statistics overview

0,07%

Found

A manageable number of counterfeit items are found in the hub.

60%

Accuracy

Countercheck has a high accuracy software. 6/10 parcels we stop are illegal.

25M€

Drugs

Per hub, we take out over €25M of drugs from communities. Protecting customers.

0.6s

Process

We do all this at an industry leading speed which allows for other ID areas.

Collaboration

SOLUTION

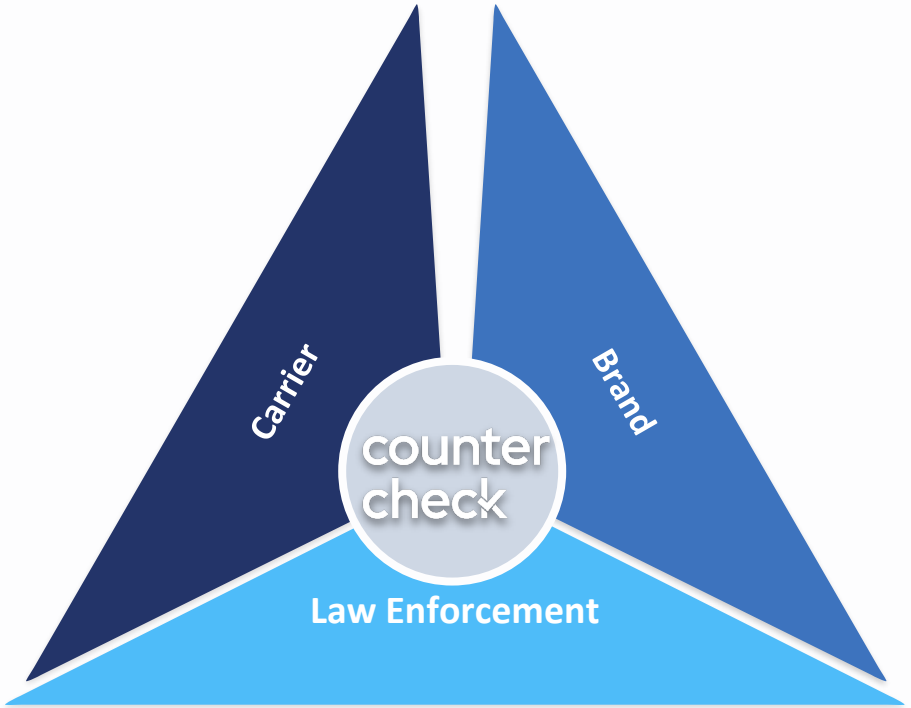
Connecting all stakeholders on one platform

Brands: Existing data from IPR holders, including counterfeit references, to train our AI monitoring technology.

Logistics: Software locally installed with carriers, establishing a software layer to analyze parcels at the point of sortation.

Authorities: Local authorities to ensure a proper procedure for opening parcels and to seize counterfeits.

Efficient identification of suspicious goods, quick confirmation of counterfeits by IPR holder => contribute to the integrity of the supply chain



Collaboration is key!

Building a safe ecosystem with no space for counterfeiters

A new standard in ***social and business responsibility*** for consumers and logistics

Efficient and ***risk analysis based check*** of entire parcel flow.

Real time control of supply chain.

Rich ***source of intelligence*** for further investigation of ***criminal networks***.

Global firewall around the region for highly dangerous consumer goods.

Join forces of all actors in Brand Protection for more ***powerful impact***.

Thank You

Karolina Zhytnikova
karolina@countercheck.com
www.linkedin.com/in/karolina-zhytnikova

Countercheck
Kollwitzstraße 64, Berlin, 10435
countercheck.com

Follow us on:

UNIVERSAL MUSIC GROUP

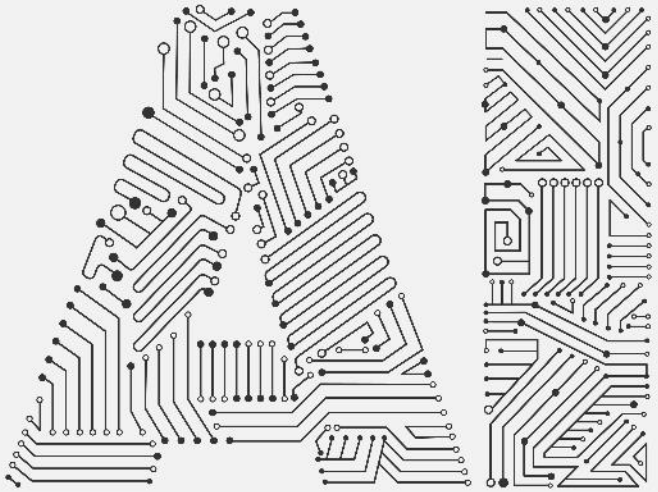
Artificial Intelligence In The Music Industry:

Its use by pirates and right holders

WIPO/ACE/16/15
Geneva, Switzerland

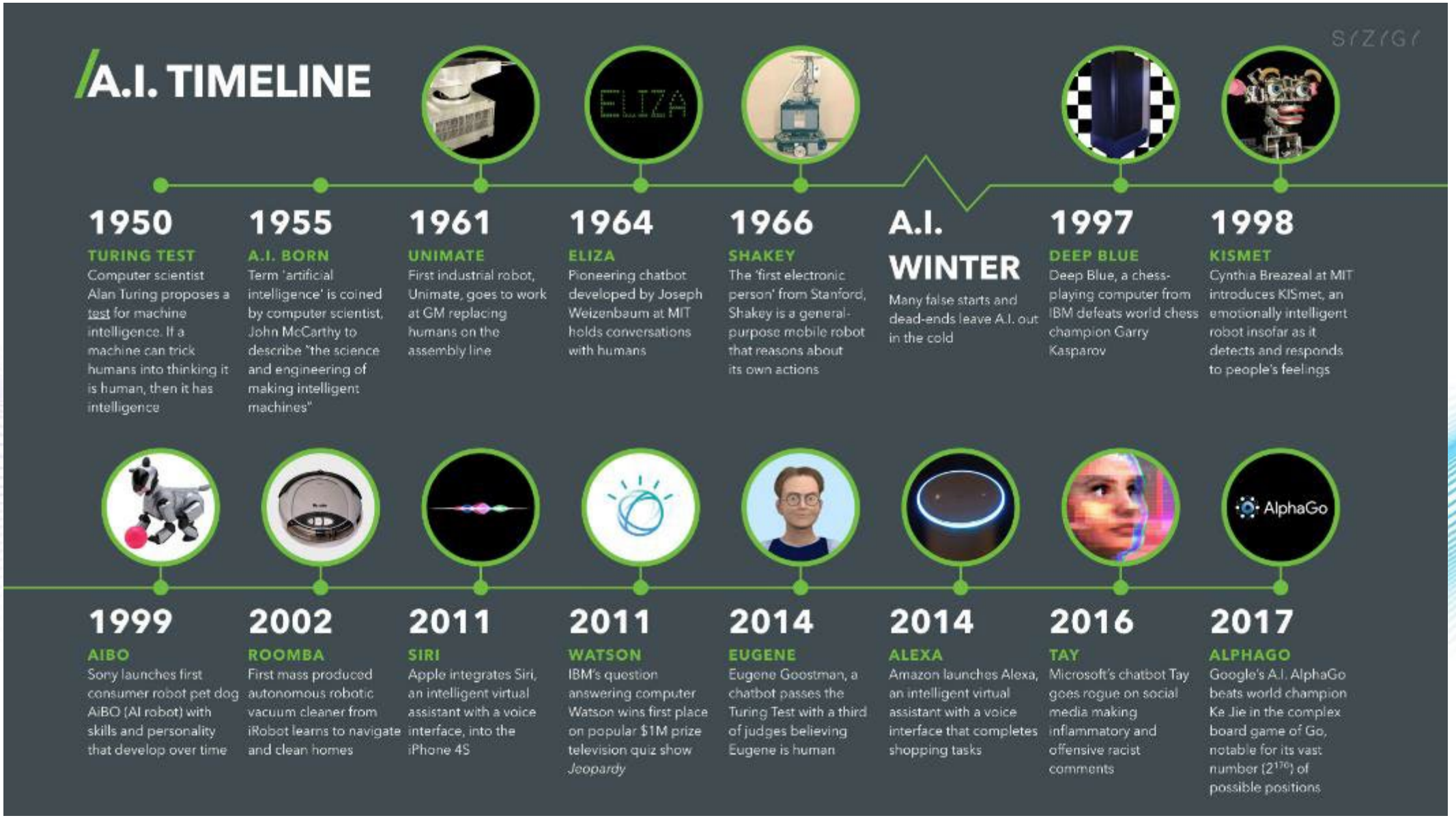
Music is storytelling

- Recorded Music
- Music Publishing
- Merchandise
- Audiovisual Experiences
- Health & Wellbeing



UNIVERSAL MUSIC GROUP

- Marketing
- Audience Engagement
- Optimizing Production
- Creative Process



Source: https://digitalwellbeing.org/artificial-intelligence-timeline-infographic-from-eliza-to-tay-and-beyond/

Created using DALL-E with the prompt "*Create an image of the world intellectual property organization and enforcement*"

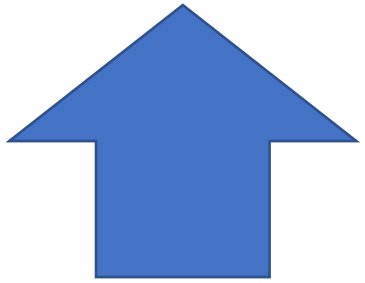
Reduced Barriers

Great Opportunity

Possible Major Risks

Trends

+175%



Unauthorised AI Generated Uploads
(Since Aug 2023)

47% Copyright

53% Name, Image, Likeness

AI generated voice over master instrumental.

Use of stream ripping & source separators

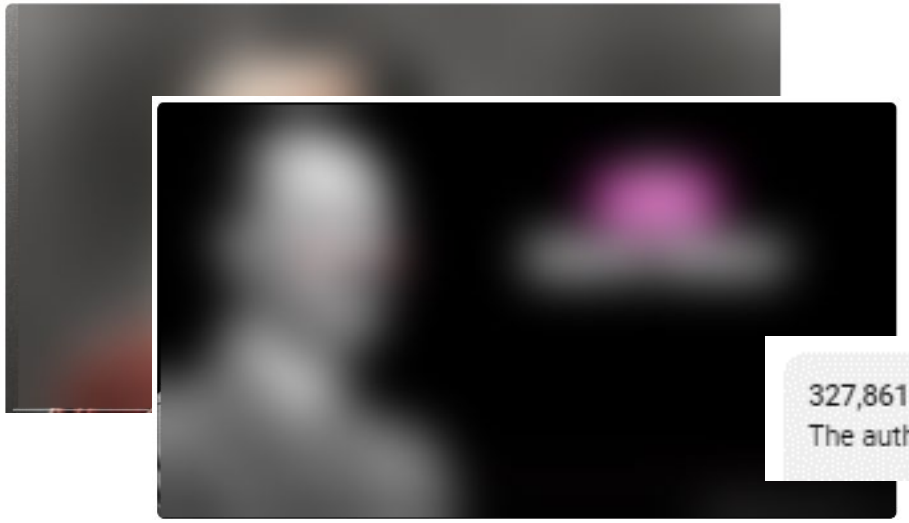
Large communities

DSPs Exploited

Example:

Original: Queen– Bohemian Rhapsody

Uses AI generated vocals of The Beatles without authorization

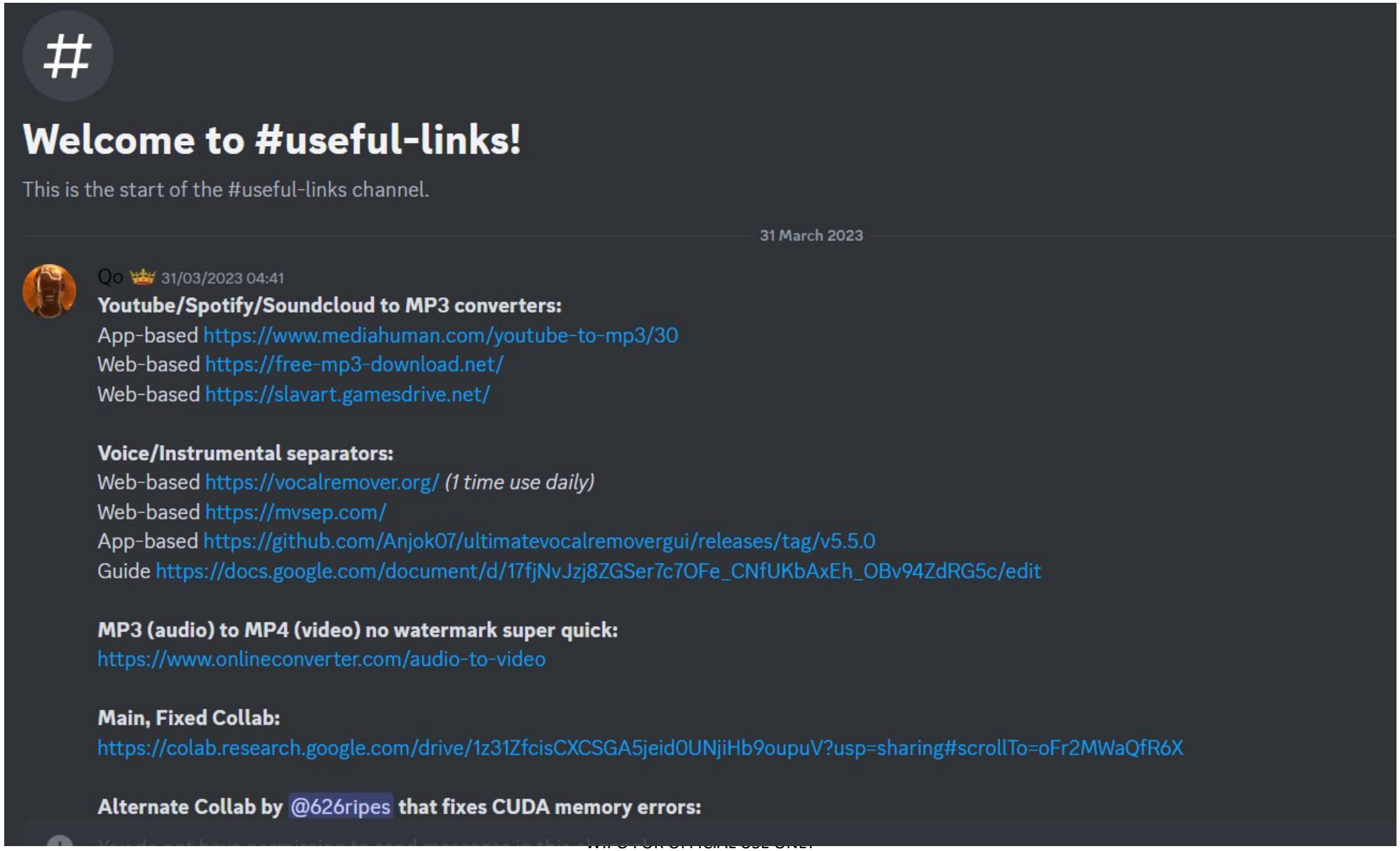


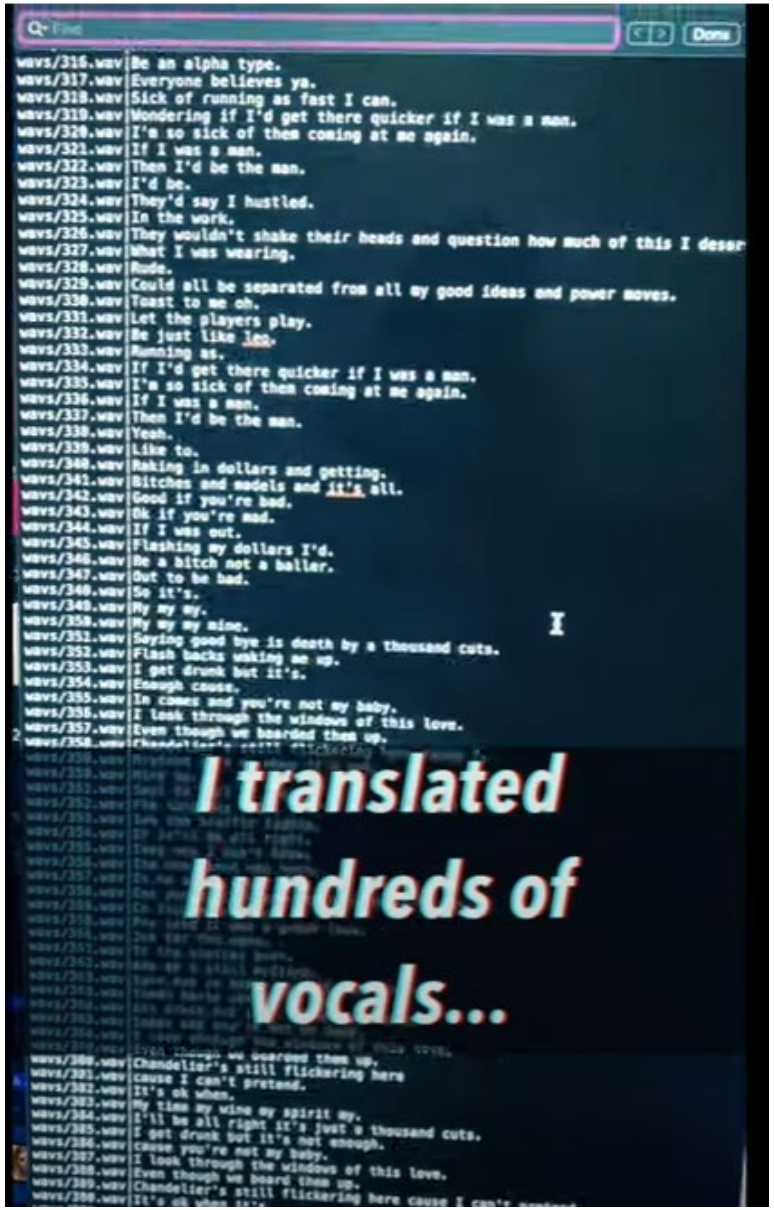
Example:

Uses AI generated vocals of an historical figure on top of the original instrumental.

327,861 views Oct 16, 2023
The author of this video despises the ideas of Nazism. This video does not intend to offend or otherwise offend other people.

AI Community Example





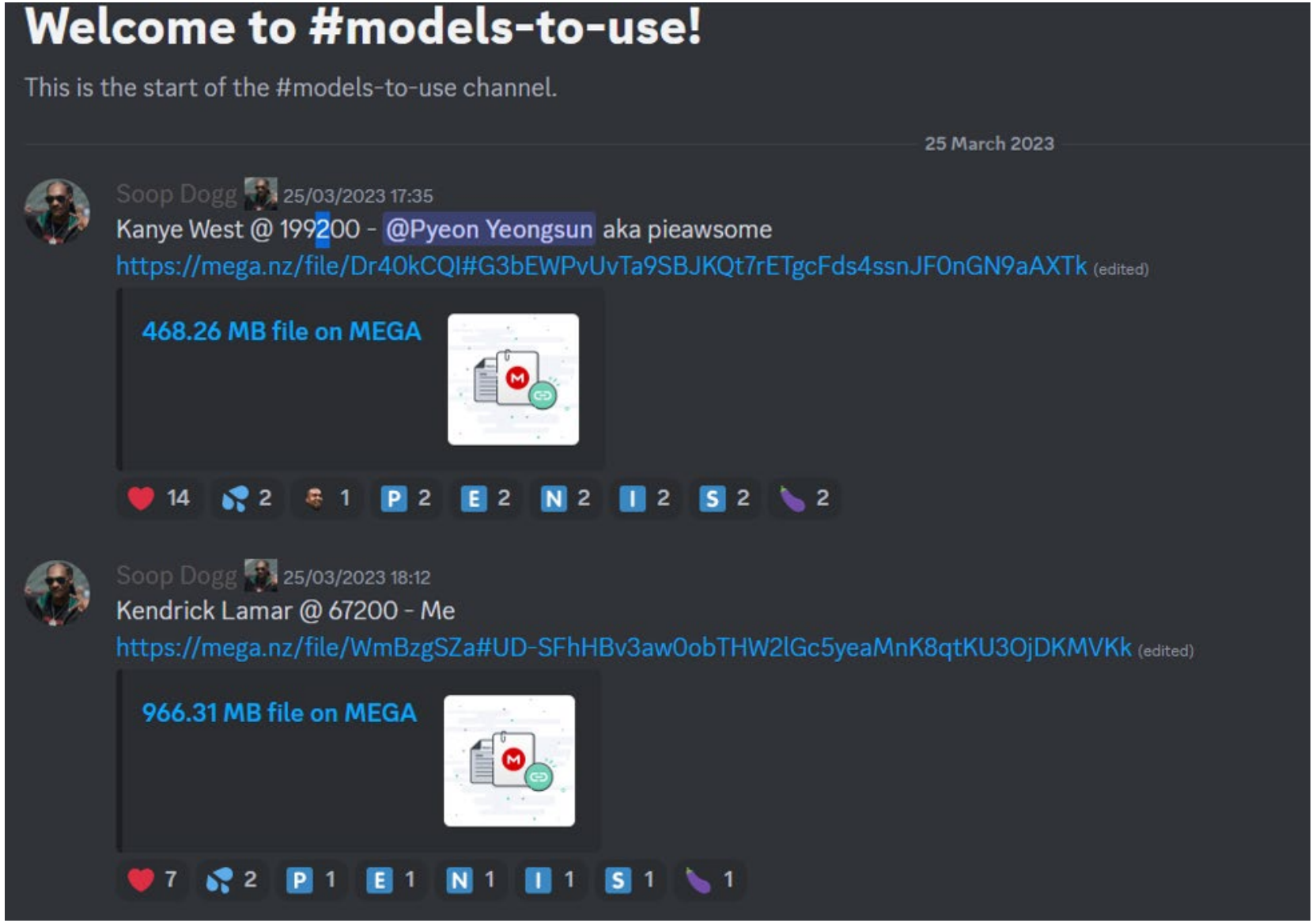
A tweet showing the training of hundreds of individual sound files being mapped to lyrics to train a vocal model

Some AI vocal models are trained on UMG master recordings

Completed models are advertised and shared across communities (Discord / Reddit etc).

Alongside tutorials

Vocal Model Example



Vocal Model Example 2

created by foxie#3461 **Join the AI Hub: https://discord.gg/aihub** **So-Vits AI: https://rb.gy/7937k Train your own model:**

Artist	Notes / Credit	Steps	Link(s)
Kanye West ⭐	Pyeon Yeongsun#5759 aka pieawsome	**199.2k**	https://mega.nz/file/P7hWwCoQ#s0OlCnRbTpcUjUlS7iQPlIYwBVeIZXzm_-1LLPSUd2Y
Kanye West (alt)	Pyeon Yeongsun#5759 aka pieawsome	**100k**	https://mega.nz/file/WmBzgSZa#UD-SFhHBv3aw0obTHW2lGc5yeaMnK8qtKU3OjDKMVKk
Michael Jackson	clubbedsam#4419	**83k**	https://mega.nz/file/wdt0iSlC#aF7pGhQr7ggBkNxu7sjExqvH3i7BtfJr3D5nPKdlNZQ https://drive
Rihanna	Seif#3218 and Provindo#4444	**200k**	https://mega.nz/file/gqYwSTaA#1Y1PFtMQLL3mkzAxLpN5HPeKhKPH_G_Nv1Zwk8F5Nbo
Rihanna (alt)	Seif#3218 and Provindo#4444	**75k**	https://mega.nz/file/UVgHBKDR#lD7bhk9XL5l-JaeyKy5mTLkqIkVe_hc0Nh1W4lMx\ https://drive
Drake	Snoop Dogg#8709	**100k**	https://mega.nz/file/Sm53wAwl#4PmlrSWDrEP1-pnZb5MJpTcfoHy3OBhBOhn2FVxfyb8
Kendrick Lamar	okcool#5237 (might be overtrained)	**1002k**	https://mega.nz/file/nlsGVKgL#9UyS-tTBC_2HH-a8MUzhDiqYBQZm7sHVRuMqvRD_-ac
Kendrick Lamar (alt)	Snoop Dogg#8709	**67.2k**	https://mega.nz/file/WmBzgSZa#UD-SFhHBv3aw0obTHW2lGc5yeaMnK8qtKU3OjDKMVKk
86k	sneakerbotter916#1658	**209k**	https://mega.nz/file/pQkhkBAS#g9HruRQAogVzprk25i9BDRrQU3Lg4tv9Yver9tHGDdU
Eminem (General Model)	Bowl#2016	**86k**	https://drive.google.com/file/d/1KVUMEEX4aTR5S-I1Chv4SO63SyoKKcv8/view

Heart On My Sleave

> AI Drake and The Weeknd: Song called Heart On My Sleeve - made with cloned voices - removed from streaming services
>
> The song, created by artist Ghostwriter, instantly went viral online for using AI-generated vocals of the Hotline Bling hit-maker, Drake, and Starboy singer The Weeknd.

Uploaded to major DSPs as “Drake & The Weeknd”

Track modified to hinder takedown efforts.

Image Sources: https://news.sky.com/story/ai-drake-and-the-weeknd-song-called-heart-on-my-sleeve-made-with-cloned-voices-removed-from-streaming-services-12859951 / https://en.wikipedia.org/wiki/Heart_on_My_Sleeve_%28ghostwriter977_song%29

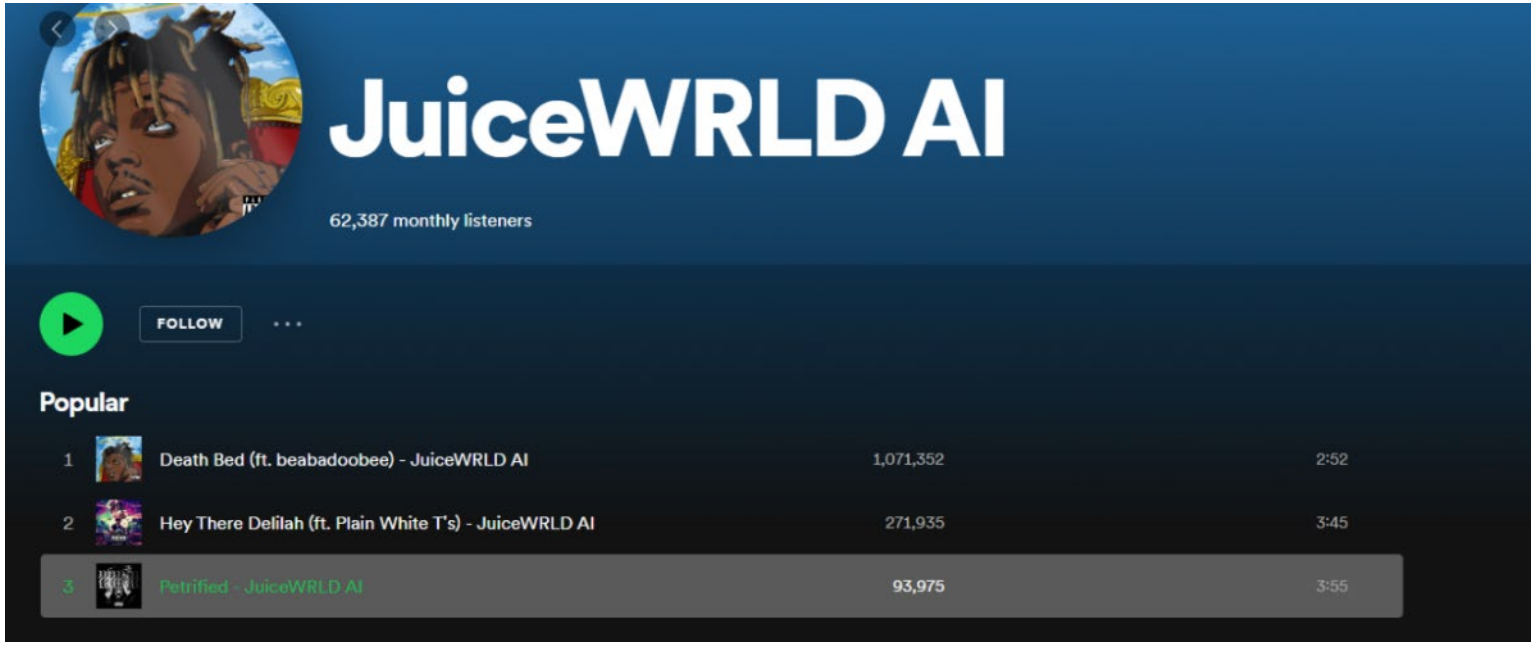
Fraudulent Tracks

Snippets of fake “hacked” tracks are created.

Full track offered for between $5k - $30k on “leak” sites.

Users are unaware track is AI generated

Digital Service Providers



Tracks are uploaded to fake accounts passing off as official to generate revenue.

Number of AI tracks uploaded increased from 50 to 400 per day.

Cyberattacks

Experts say AI scams are on the rise as criminals use voice cloning, phishing and technologies like ChatGPT to trick people

ChatGPT tool could be abused by scammers and hackers

An unusual case of CEO fraud used a deepfake audio, an artificial intelligence (AI)-generated audio, and was reported to have conned US$243,000 from a U.K.-based energy company. According to a report from the Wall Street Journal, in March, the fraudsters used a voice-generating AI software to mimic the voice of the chief executive of the company's Germany-based parent company to facilitate an illegal fund transfer.

AI based phishing tools (i.e. FraudGPT) can be used to obtain pre-release tracks or other audio.

Deepfake audio can be used to deceive

Examples uses

DOLBY ATMOS™

INGROOVES MUSIC GROUP

Endel

UMG uses AI in many ways

- **The Beatles** – Helping restore life to old demo recordings
- **Studio Tool** – Creation of drum tracks and assist with chord progressions.
- **Apps** – Health & Wellbeing
- **Data** – Help identify trends in data and assist with decision making.
- **Engagement** – Helping our fans discover new artists and music.

AI in the detection of counterfeits

To date we have detected **over USD$45m+** of counterfeit products using AI.

AI compliments our efforts through the identification of our trademarks even when distorted or deliberately altered.

The vast amount of counterfeit merchandise across multiple jurisdictions and sellers make this an endless task without the use of AI.

Counterfeit sales are linked with serious organised crime, health & safety and identity theft.

AI Regulation

- In general, UMG believes that the current copyright legislation, if interpreted, applied and enforced correctly, does not need to change.

- However, in selected territories additional protection of personal rights (i.e. voice and likeness) may be necessary.

Conclusion

AI in the service of artists and creativity can create some wonderful tools.

We work with numerous companies, platforms, artists and creators who use AI in a responsible way.

AI that is used to undermine the legitimate use of music, unjustly influence or uses an artists name, image, likeness or voice without authorization is not ok.

UNIVERSAL MUSIC GROUP

Thank You

Graeme Grant
Vice President, Global Content Protection
Universal Music Group
Graeme.Grant@umusic.com

Robbert Baruch
Senior Vice President, Public Affairs Europe
Universal Music Group
Robbert.Baruch@umusic.com

Use of AI to detect and remove offers of Counterfeit Goods

February, 2024.

01

Regulatory Context in Latam

Current Status

Intermediaries Liability

- Chile (2010)
- Costa Rica (2011)
- Paraguay (2013)
- Brazil (2014)
- Mexico (2020)
- None includes a general monitoring obligation.

Artificial Intelligence

- No governing regulation. Some bills of law in few countries.

02

How we fight offers of counterfeit products

Mercado Libre self-regulated solutions to **fight offers of counterfeit and pirated goods**.

Proactive

Collaboration Agreements with the private and public sectors, cooperation with the authorities and partnerships with the brand owners

Proactive removals of infringing trends and patterns

- Based on learnings from notice submitted through NTD mechanism.

Brand Protection Program (BPP)

- Notice and Takedown (NTD) mechanism in which the listing is not reinstated after a counter notification.
- Possibility to enforce any IPR, namely, trademarks, copyrights, related rights, patents, utility models, industrial designs and plant breeders rights.
- Policies that provides information on IPR and how to avoid infringing third parties rights.

Reactive

03

AI as a Tool for Proactive Detection

Massive Data

45

PURCHASES

Per second

+140

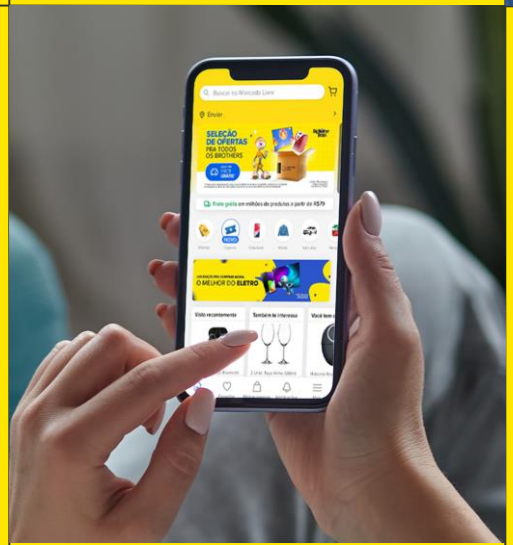
THOUSAND

Listings created or edited per hour

3.3

MILLIONS

Unique sellers



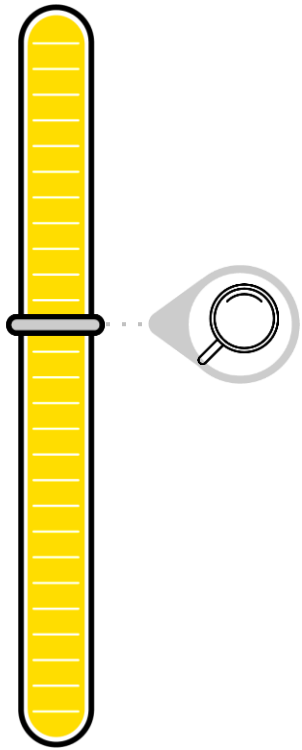
50.3

MILLIONS

Unique buyers

Machine Learning/ Artificial Intelligence solutions to **fight offers of counterfeit goods**.

Proactive



Reactive

Proactive removals of infringing trends and patterns

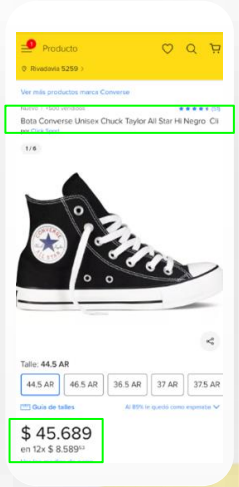
Proactive Listing Removal
Evidence of counterfeit goods in new listings.

Brand Detection
Text and logo on a listing.

Compatibility
Seller's possibility to edit its listing to include true statements indicating compatibility with branded products.

Customer feedback detection
Q&A, reviews, claims.

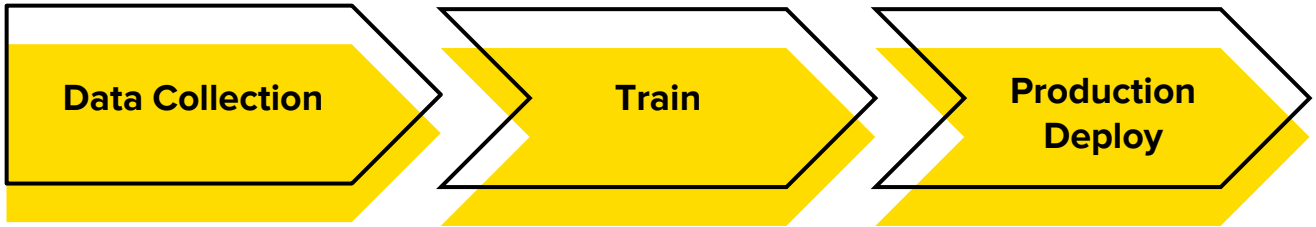
Evidence AI searches on a listing



Semantic Algorithms

Logo Detections

Proactive Model Development Process



- IPR owners notices.
- Manual labeling.
- Weak labeling.

- Features exploration.
- Supervised learning.
- Predictive classification.

- Novelties flow (+90M/month).
- Response Time <400 ms.
- Monitoring (RR, FN)

04

Results

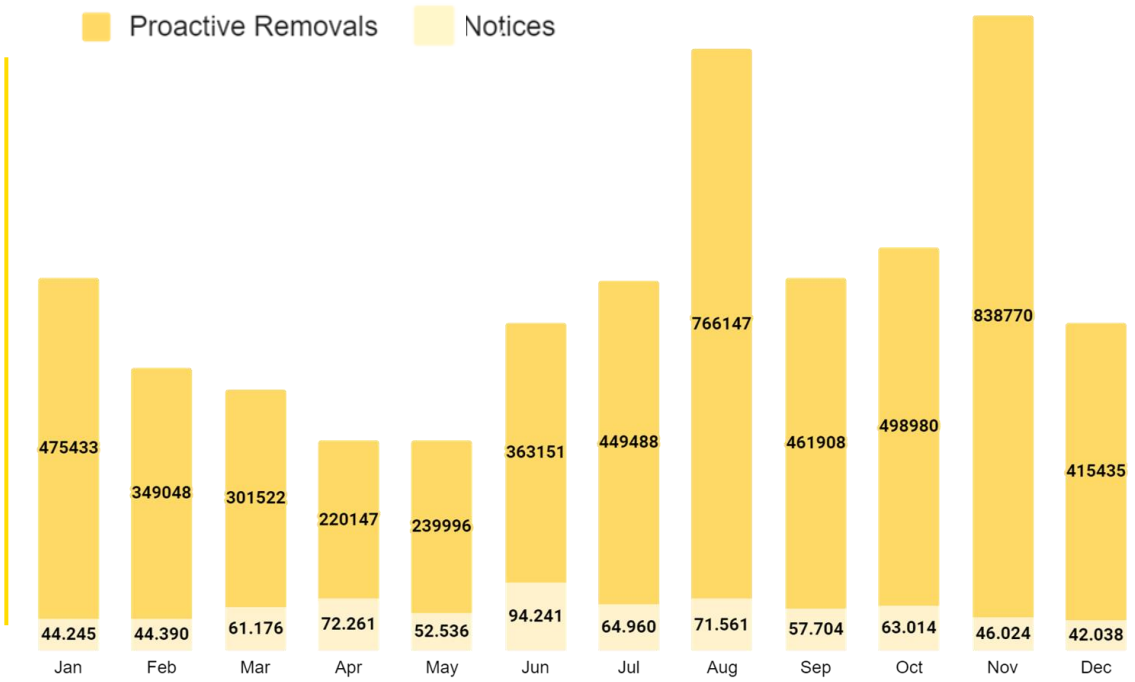
2023 BPP takedown requests and proactive removals

+714K

Takedowns based on notices submitted by BPP participants

+5.3M

Proactive removals

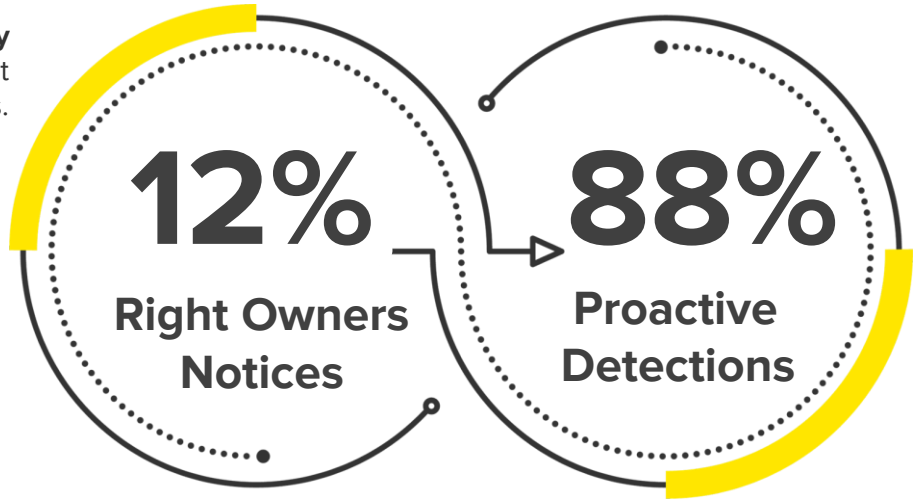


For each IPR holder notice submitted through the BPP

Mercado Libre proactively removed almost 8x as many listings.

Teamwork

An **effective and friendly tool** to monitor and report infringing listings.



We learn about infringing trends from IPR owners' notices to proactively remove listings including those patterns.

For each requested delisting or proactive detection, the system triggers a **behaviour seller analysis** to determine whether an additional sanction should be applied to the seller: **warning, suspension or permanent restriction to sell**.

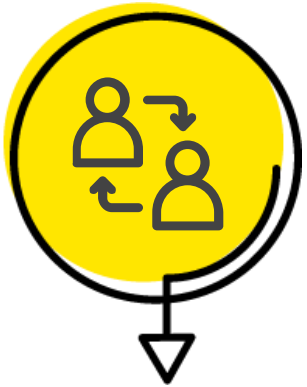
05

Challenges

Ongoing Challenges

Higher participation of IP owners in reporting through NTD mechanisms would imply **better knowledge** on infringing trends.

While **market price of original products** could provide a benchmark for detection, it **cannot be the only** basis for identifying counterfeit products.



Need of **continuous learning** to deal with **constant sophistication** of infringers.

THANKS