

Online Intellectual Property Crime:

Recognising the Threats from Emerging Technologies Taking AI as an Example

7 March 2023

John ZACHARIA, Zacharia Law PLLC
Erling VESTERGAARD, Observatory, EUIPO

PROGRAMME

Online IP Crime and AI

- Intellectual property crime landscape
- Emerging and disruptive technologies
- Artificial intelligence
- IP crime threats fueled by AI
- Take-away points
- Learn more

Post your questions or comments in the chat anytime and we will try to answer!

Before we begin – a rhetorical question

What do Oedipus, Harry Potter, Snow White, Macbeth and Morpheus (Matrix movies) have in common?

- Fully or partially fictional characters, yes;
- But in behaviour they are all motivated (sometimes to the level of obsession) by **prophecy, prediction**.
- **Prediction** is the process of filling in missing information to support **decision** making.
- AI applications are **prediction machines**.
- **Prophecy**: AI will be a component of all online IP crime and most other online crimes within 5 years (if not already).



Intellectual property crime landscape

General online crime threats

- Online environment is effectively used to **upscale** crime.
- Crime can easily be carried out at **a distance**.
- Anonymisation tools are widely used to **obfuscate** crime.
- Online crime poses a number of **jurisdictional challenges**.
- **New criminal structures** (swarms and hubs) and modus operandi ('crime as a service' and dark web) are evolving.
- **Anti-forensic strategies** are extensively applied.
- **Multitude of targets**: vulnerable internet users SMEs, business emails and e-commerce.

Main types of IP crime

- **Production, import and wholesale** of IP infringing goods (domestic production, re-working and large-scale imports).
- **Marketing and distribution** of IP infringing goods (sales on social media platforms, e-commerce platforms and infiltrating the legal supply chain).
- **Live streaming** (subscription or advertising-based IPTV crime).
- Distribution of **copyright protected materials** (VOD).
- IP registration and services **fraud** (trade mark invoice fraud).
- **Cybersquatting and typosquatting** (phishing, spoofing and malware injection).
- Trade secret **theft** (cyberattacks and ransomware).

2 Emerging and disruptive technologies

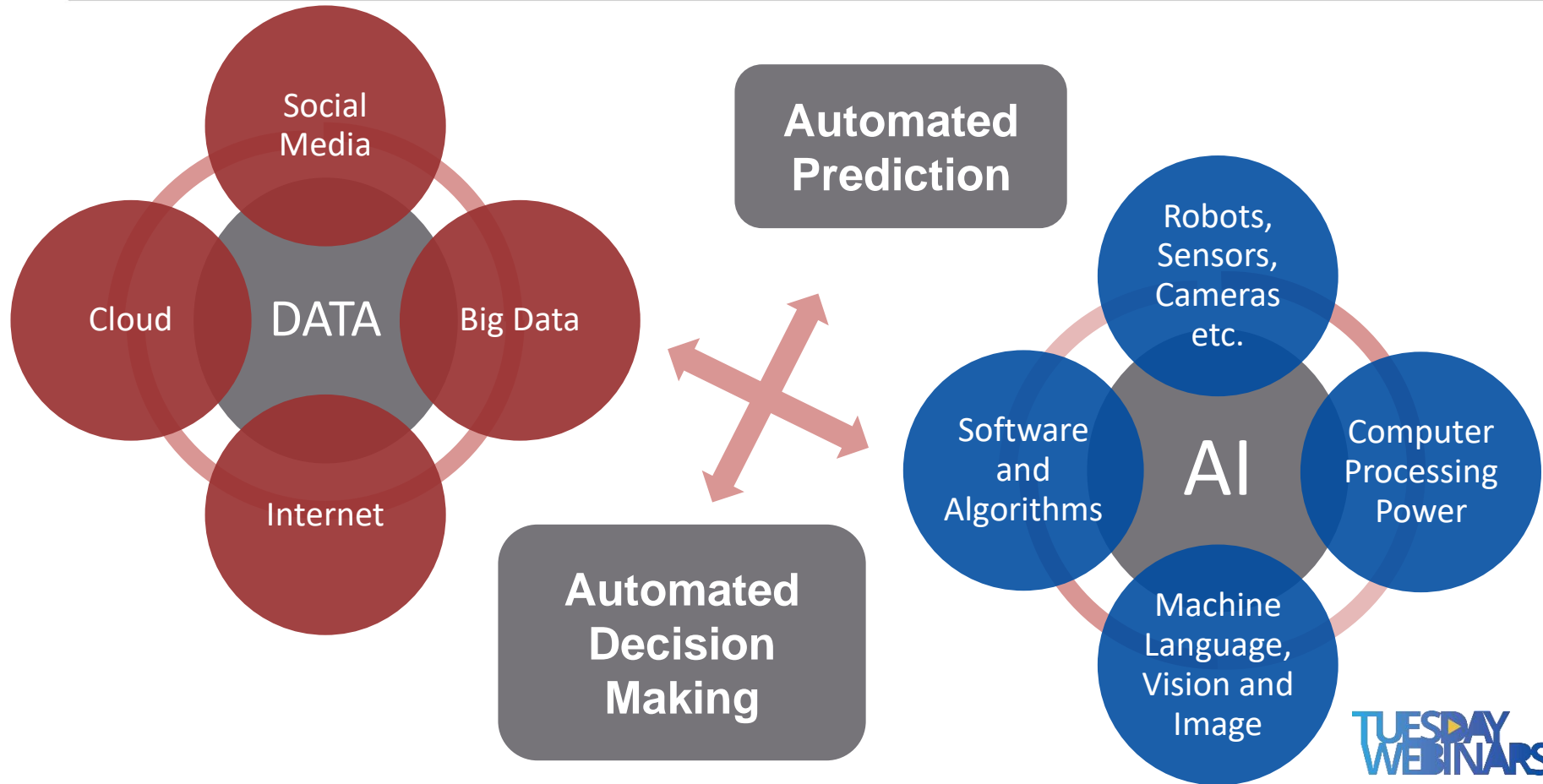
Technological trends

- New **material** technologies (robotics and nano-tech, 3D printing).
- Augmented, mixed and virtual **reality** (Metaverse).
- **Internet enhancing** technologies (5G/6G mobile networking, edge computing and cloud services).
- **Cybersecurity and big data.**
- **Blockchain** and distributed ledger technology (cryptocurrencies, non-fungible tokens (NFTs) and smart contracts).
- **Quantum computing.**
- **Artificial intelligence.**

3 Artificial intelligence

Concept of AI

Computer code (software and hardware) that, according to algorithmic rules, dynamically adapts as large datasets are processed with the aim of predicting phenomena and assisting decision making.



ARTIFICIAL INTELLIGENCE STREAMS & TECHNIQUES

Artificial Intelligence (AI)

STREAMS

Machine Learning

Deep Learning

Natural Language Processing

Expert Systems

Computer Speech

Computer Vision

ALGORITHMS

Advanced algorithms

Neural networks

Generative adversarial networks

...

OTHER APPLICATIONS

Quantum Computing

Robotics

IoT

...

AI-related general crime threats

- Convincing **social engineering** attacks at scale
- **Document-scraping** malware to make attacks more efficient.
- **Evasion** of image recognition and voice biometrics.
- **Malware** development, testing and optimisation.
- **Ransomware** attacks, through intelligent targeting and evasion.
- **Data pollution**, by identifying blind spots in detection rules.
- **Deepfakes.**

4 IP crime threats fueled by AI

Production, import and wholesale of IP infringing goods



Scenario

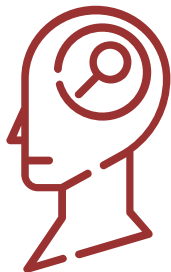
- IP criminals intend to sell infringing versions of a trade mark-protected clothing line all over the world and need to find a way of avoiding customs inspections and seizure.



IP criminals use AI to

- identify and create shell corporations in different countries;
- engage in port shopping where customs are least likely to seize **fakes**;
- **optimise concealment** of the infringing goods in shipping containers;
- find the quickest trade route between its illicit factories and ports of entry.

Production, import and wholesale of IP infringing goods



IP criminals

- can use **machine learning** to create a system that identifies the quickest trade route between its illicit factories and ports of entry, chooses ports, and helps to conceal infringing goods in containers.
- can also employ **expert systems** to optimise the decision-making process used for its supply chain.
- can utilise **adversarial machine learning** to evade detection, change trade routes and even provide deceptive input data, or ‘false flags’, to cause a malfunction in the machine learning model that customs authorities may use and make it generate inaccurate information.
- If law enforcement or customs authorities use machine learning, IP criminals could use a machine learning model extraction attack to obtain information on its functioning, as a ‘**reverse engineering**’ strategy.

Marketing and distribution of IP infringing goods



Trade mark owners

- routinely market and sell their brand name goods online through popular third-party e-commerce platforms.



IP criminals

- can use AI to scan online listings to identify a trade mark owner's most popular clothes.
- can then use this information to sell infringing versions on popular third-party e-commerce platforms.

Marketing and distribution of IP infringing goods



Machine learning, computer vision and natural language processing can all be weaponised by IP criminals to scan websites and identify the most popular designs, which they will later infringe and sell online.



IP criminals could also use AI with **virtual/augmented reality** to develop an online persona and promote infringing products on social media marketplaces. In this case, IP criminals could hide their identities while launching different marketing campaigns.

Live streaming of copyright protected digital content



Scenario

- IP criminals want to profit from fans of Mixed Martial Arts (MMA), so they use AI to create a link aggregator that finds and posts all the links that other groups have created so other fans can watch the MMA matches for free.
- They generate revenue from advertising on the website where they post the aggregated links.



Machine learning

- can be used by IP criminals to identify and scan the most popular and relevant websites, and then suggest infringing links to MMA programming.
- can also find and automatically extract the links to infringing streams, before reposting them on the IP criminals' own website.

Live streaming of copyright protected digital content



Scenario

- IP criminals want to offer access to copyright-protected television programming without having to pay the subscription fee service.
- They develop and sell an AI-enabled IPTV app that customers can buy and download onto their smart televisions.



The AI-enabled IPTV app circumvents technological protection measures, enabling purchasers to avoid paying television subscription fees and to watch all of the television programming for free.

Live streaming of copyright protected digital content



IP criminals

- could weaponise **machine learning** to identify the protection measures of a legitimate streaming service to break into the system and gain access to its content.
- Circumvention methods are then shared with the IP criminals' app customers in an adaptive way, so they can access without paying.



IP criminals could also use AI tools to identify broken links or streams with lag spikes, and then reroute the stream's source or forward a working link to the IPTV service customers.

Distribution of copyright protected digital content



Scenario

- IP criminals use AI to develop and run a decentralised file-sharing network to distribute copies of copyright-protected films. The network is connected to a cryptocurrency blockchain, enabling the IP criminals to sell premium accounts on the file-sharing network (and anonymously pay rewards to members who occasionally upload infringing content to the file-sharing network).
- They could also use AI to quickly circumvent the technological protection measures that copyright owners use to prevent unauthorised access and copying of its copyright-protected films.

Distribution of copyright protected digital content



IP criminals

- can weaponise **AI-supported blockchain** to evade detection by copyright owners.



AI-enabled machine learning

- could also eliminate digital dots and watermarks that copyright owners add to their copyright-protected films to track their films' unauthorised copy distribution online.



Generative adversarial networks

- could also be used to incorporate certain effects into livestreams to prevent automatic content recognition by adding new logos, removing original logos, watermarks and fingerprinting or enhancing content.

Trade secret theft



Scenario

- IP criminals learn that a company plans to launch a new soda line based on a secret new formula the company is developing.
- They use AI to steal the soda company's new formula, before the new soda is available to consumers.



IP criminals

- conduct AI-reconnaissance to identify the weakest employee to be duped by a phishing email: the executive assistant to the CEO of the soda company.
- AI optimises a spear phishing attempt to obtain the CEO's email credentials to send an email to the head of the soda company's development team to obtain the new secret soda formula.
- also obtained deepfake software from a Crime-as-a-Service group.
- It generates a deepfake of the CEO's voice and leaves a voicemail with the development team's lead asking to email the new formula to an email account under the IP criminals' control.

Trade secret theft



Reconnaissance is an AI-supported **machine learning** technique that learns from social media profiles, in this case by analysing the communication style of the soda company CEO's executive assistant to create an alias of a trusted individual.

Natural language processing generates text that can be used to write false emails and written communications.

AI-supported hacking, AI-supported password guessing, and AI-supported CAPTCHA breaking can be used to predict the correct password and enable the IP criminals to enter the CEO's email account.

Deepfakes of the CEO's voice in this scenario can be generated by Generative Adversarial Networks in **computer speech**.


IP rights registration and services fraud



Scenario

A soda company hopes to register a new mark to go with the new soda brand that the company is developing.

After stealing the soda formula, IP criminals steal the new mark too, so they may fraudulently register the new mark as their own trade mark.



IP criminals use AI to ‘trick’ the IP office into believing that the soda company’s original mark was actually created by the IP criminals.



IP criminals can weaponise **generative adversarial networks** and **computer vision** tools to produce a fake application for registration, replicating similar applications filed by the soda company.

Natural language processing tools could be used to replicate the text.

IP rights registration and services fraud

The soda company must pay a renewal fee to the IP registration office for its existing trade marks.



IP criminals send the soda company an invoice that looks like it came from the IP office, but includes a payment address that the IP criminals control, to receive the soda company's re-registration or renewal fee.



IP criminals can use **machine learning** with pattern recognition and **computer vision** tools to produce a fake re-registration or renewal invoice identical to the original issued by an IP office.

Natural language processing can be employed by IP criminals to create text that resembles an authentic invoice or other 'official' document.

Cybersquatting and typosquatting



Scenario

IP criminals:

- use AI to quickly identify the most popular brand name in companies that have not yet registered all of their popular trade marks as domain names.
- then register, or 'squat', on these trade marks as domain names that the IP criminals own.

Then they sell goods bearing counterfeit versions of the trade marks in the domain names that the IP criminals control.



They can use **machine learning** to identify the most popular brands not already registered as domain names and create domain names that incorporate these trade marks into new domain names that the IP criminals would then register.

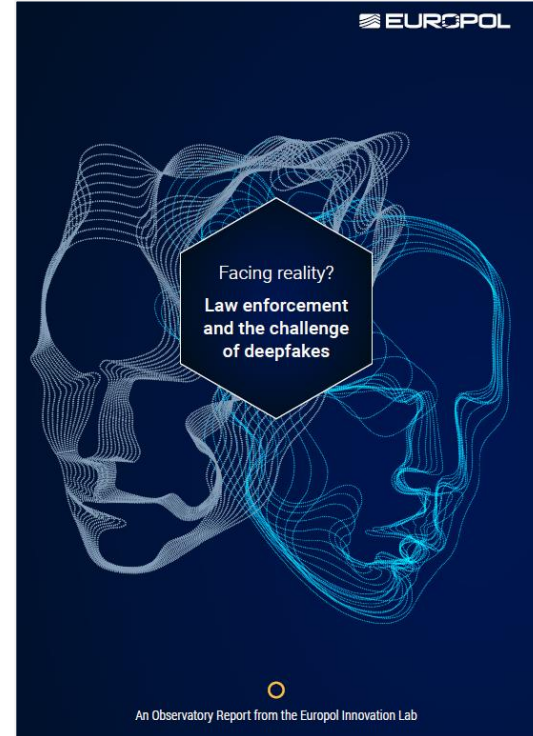
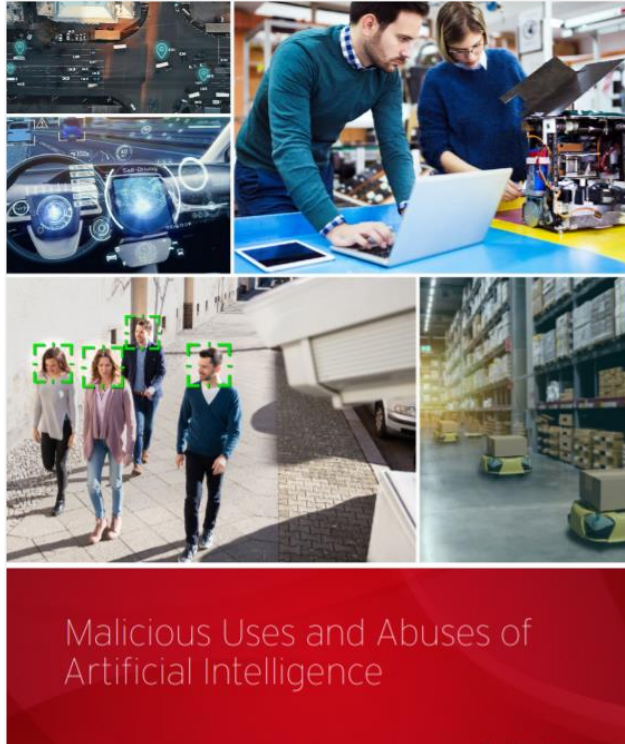
5 Take-away points

AI is strong facilitator of IP crime due to

- **Anonymisation** capabilities.
- Well suited for **scalability**.
- Ability to overcome **proximity**.
- Makes **jurisdiction** more difficult to define.
- Increasingly **user friendly** for criminals.
- Strong for **anti-forensic strategies**.
- Facilitates new ways of **cooperation**.

6 Learn more

Great resources of knowledge



Great resources of knowledge



Impact of Technology Deep Dive Report I

STUDY ON THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE INFRINGEMENT AND ENFORCEMENT OF COPYRIGHT AND DESIGNS



OBSERVATORY



Intellectual Property Infringement and Enforcement Tech Watch Discussion Paper 2023

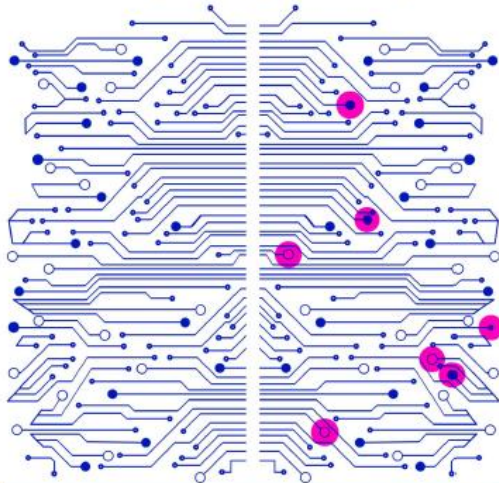
Prepared by the European Observatory on Infringements of Intellectual Property Rights, EUIPO, with support from the Impact of Technology Expert Group



Great resources of knowledge



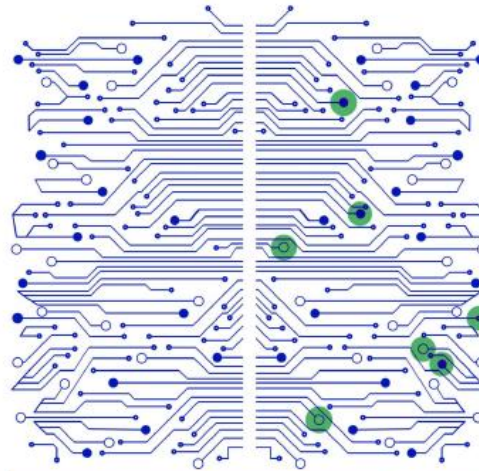
Automated Content Recognition:
Discussion Paper – Phase 1
'Existing technologies and their impact on IP'



November 2020



Automated Content Recognition:
Discussion Paper – Phase 2
'IP enforcement and management use cases'

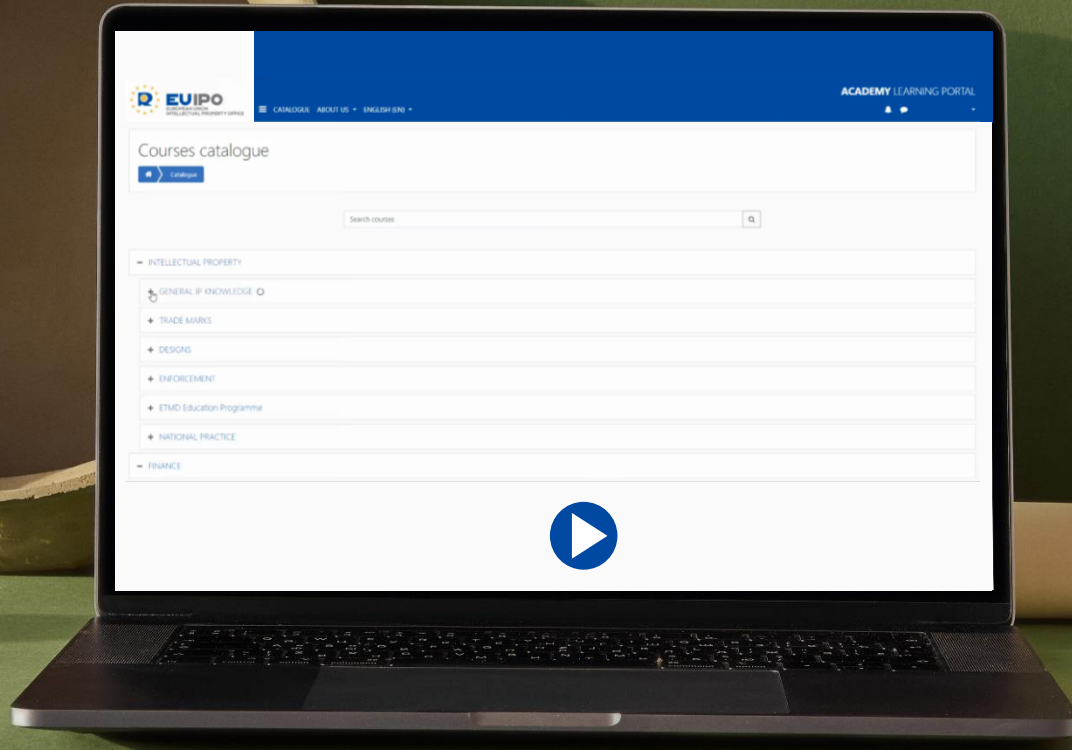


September 2022





Keep in touch with the EUIPO Academy





EUIPO

EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu



[@EU_IPO](https://twitter.com/EU_IPO)



[EUIPO](https://www.linkedin.com/company/euipo)



[EUIPO.EU](https://www.facebook.com/EUIPO.EU)

THANK YOU



John ZACHARIA
Zacharia Law PLLC
john@zacharialaw.com

Erling VESTERGAARD
EUIPO Observatory
erling.vestergaard@euipo.europa.eu

