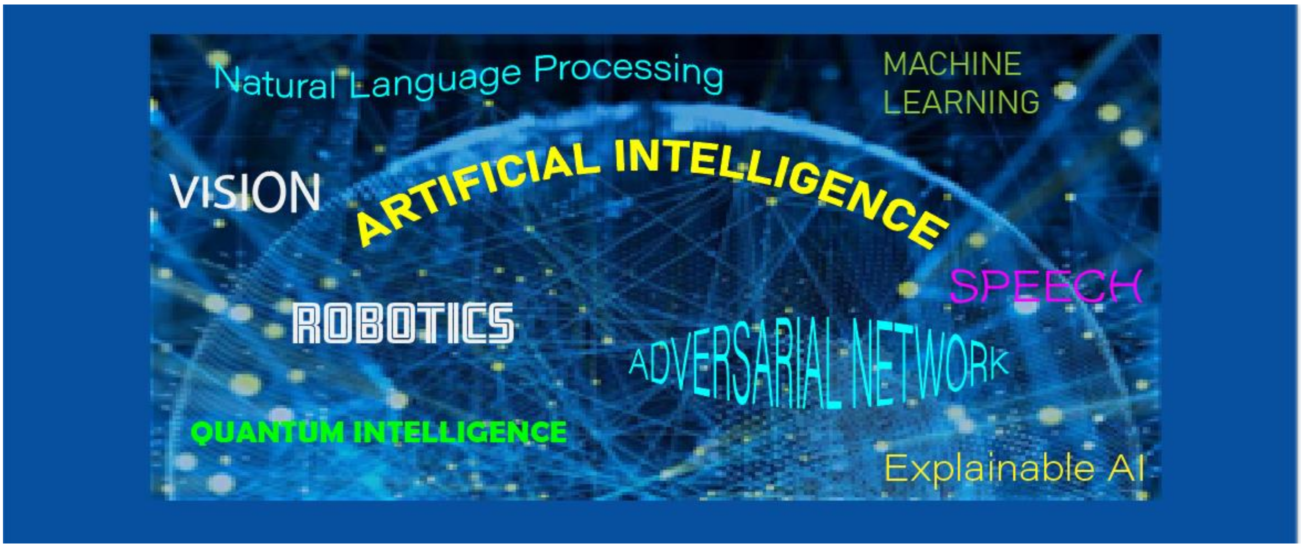
EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

Impact of Technology Deep Dive Report I

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

Executive Summary



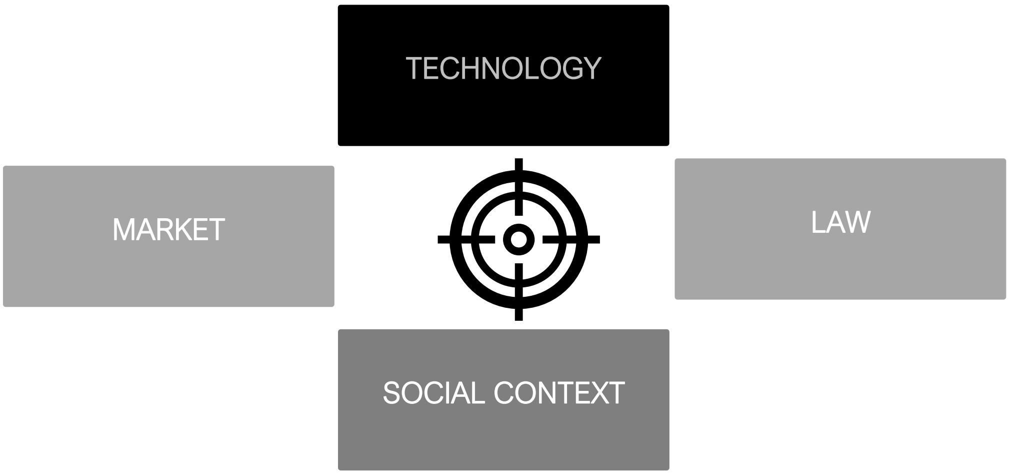
March 2022

Executive Summary

Background

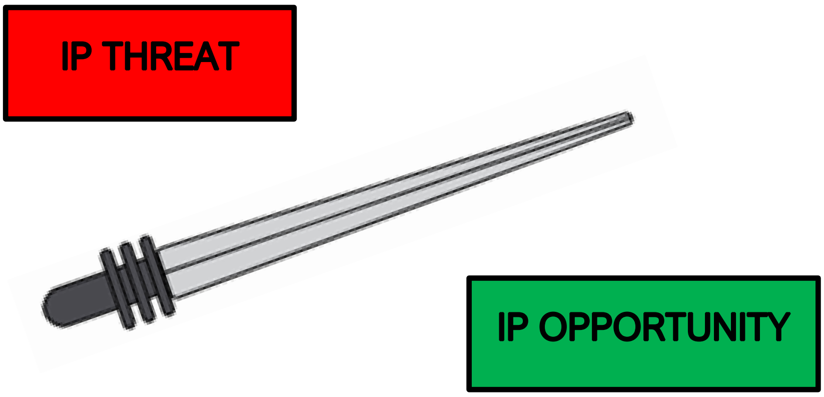
In early 2019, the European Union Intellectual Property Office (EUIPO) established an Impact of Technology Expert Group (EG). The group is composed of experts with knowledge of and practical experience in monitoring the impact of new and emerging technologies on the infringement and enforcement of intellectual property rights. The EG follows a specific approach based on an adaptation of Lawrence Lessig's 'Code and Other Laws of Cyberspace' theory (the Code Theory), which describes how human online activity is regulated by law, social norms, and the market, taking into consideration the internet's technical infrastructure (referred to as 'code'). The Code Theory has been adapted by the EG in the sense that it believes all technological impact on intellectual property should be considered from four angles: the market; the law; the social context; and the technology itself.

Expert Group's adaptation of Lessig's Code Theory



The approach followed in analysing the impact of new technologies on IP can be described using the 'double-edged sword' metaphor shown in the figure below. The starting point is the consideration that the use of a particular technology either to infringe IP or to protect and enforce them presents, to some extent, the same features in each case. This metaphor also suggests that there may be weaknesses in the application of technologies on each side that can be exploited by the other.

The 'double-edged sword' metaphor



The EG developed a unique methodology called the 'Intellectual Property Tech Chain', which is described in detail in its first report, published in September 2020, entitled 'Intellectual Property Infringement and Enforcement Tech Watch Discussion Paper 2020'. According to this methodology, the development of any application follows four steps:

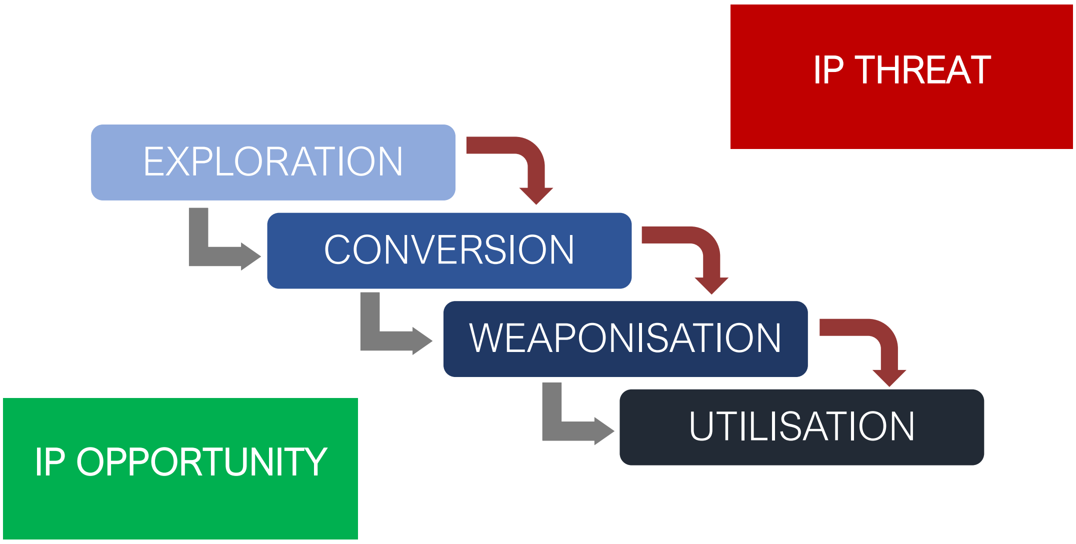
- **exploration**, i.e. assessing the technology to ascertain whether it could be used to infringe or protect/enforce IP;

- **conversion** of the technology to enable the achievement of the identified goal;

- **weaponisation**, i.e. finalising the application's development;

- **utilisation**, i.e. actual monetisation or use of the application to infringe or protect/enforce IP.

The ‘Intellectual Property Tech Chain’



In 2021, the EUIPO commissioned the United Nations Interregional Crime and Justice Research Institute (UNICRI) to carry out the first deep-dive research project applying this methodology in cooperation with the Impact of Technology Expert Group.

The current crime landscape was considered when drafting this study. The yearly strategic Internet Organised Crime Threat Assessment (IOCTA) report, produced by Europol’s European Cybercrime Centre (EC3), provides an overview of the emerging threats and developments in the cybercrime landscape. In 2020, the highest-priority threats included social engineering, ransomware, and other forms of malware. It is essential to consider the impact of the ‘cyber-’ element of cybercrime when analysing criminal activity, since it frequently has a bearing on nearly every aspect of this activity. In the recent IOCTA 2021 report, Europol listed the ransomware affiliate programs using supply-chain attacks to compromise the networks of large corporations and public institutions and deploy new multi-layered extortion methods, overlayered mobile malware attacks, and distributed denial of service (DDoS) for ransom. Chapter 5 of this study will explain how these threats are also relevant in the context of copyright and designs.

The development and evolution of cybercrime must also be considered in conjunction with the misuse of AI, including in AI-facilitated IP crime. The emerging malicious use of AI can enhance the impact of cybercrime since it is able to perfect social engineering attacks at scale and, among others, it can be used:

- for document-scraping malware to make attacks more efficient;
- to evade image recognition and voice biometrics;
- to create ransomware attacks through intelligent targeting, evasion, and data pollution by identifying blind spots in detection rules;
- to improve blockchain capabilities in online crime.

The relevance of addressing IP crime has also been raised as a priority in the current context. In May 2021, the EU's Council of Ministers included IP crime among the top 10 priorities in the fight against organised crime to be addressed in 2022-2025. On 26 May 2021, the Council adopted the conclusions setting the 2022-2025 EU priorities for the fight against serious and organised crime through the European multi-disciplinary platform against criminal threats (EMPACT).

In this context, this study aims to provide an assessment of the impact of AI technologies on both the infringement and enforcement of copyright and designs.

Methodology

The purpose of this study is to analyse the impact of AI technologies on both the infringement and enforcement of copyright and designs. These have much in common with the infringement and enforcement of other IPs (e.g. trade secrets, trade marks, and patents) through the application of AI, but this study will not take these other types of IP specifically into consideration.

This study is meant as a practical, practitioner-oriented tool to help understand the impact of AI and put this impact into a broader perspective. To this end, 20 scenarios have been developed to demonstrate existing or potential misuse of AI technologies to infringe copyright (and related rights) and designs, as well as the use of AI to enforce these same rights. The focus of enforcement of the selected IP is the application of AI in the field of law enforcement. However, there are, and will be in the future, many relevant applications of AI that overlap or have many commonalities with voluntary enforcement measures, civil enforcement, and certain aspects of administrative enforcement.

The data collection encompassed a variety of elements: a desk review study; interviews and focus group discussions; and case analysis. At the start of the project, the EUIPO facilitated contact with a broad group of experts (including the Impact of Technology Expert Group), who were invited to contribute to and support the research. The researchers then contacted other experts to supplement the information thus obtained.

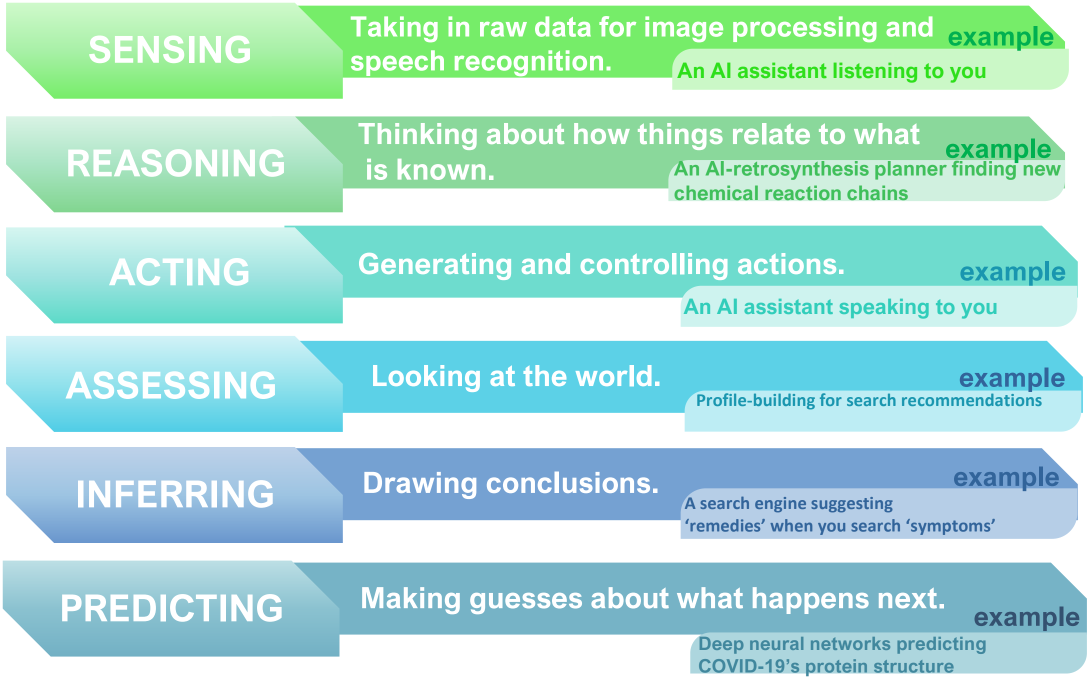
Generally, experts were identified based on their knowledge of and experience with AI technologies themselves, the copyright and design infringement and enforcement landscape, and (in particular) issues surrounding the application of AI in the infringement and enforcement of copyright and designs. Many of the experts reviewed and commented on the methodology of the study, and all of them actively supported the research, including through participation in group discussions and online interviews and, whenever possible, providing case studies.

Key findings

AI technologies have passed through different phases since their initial development, dating back to the late 1940s and early 1950s, but there is still no widely agreed-upon and precise definition of what AI is. It is commonly understood as a subfield of computer science focusing on developing computer systems that can perform tasks that would normally require human intelligence.

AI has various capabilities, from sensing, reasoning, and acting to assessing and even predicting.

AI Capacities



SENSING

Taking in raw data for image processing and speech recognition.

example

An AI assistant listening to you

REASONING

Thinking about how things relate to what is known.

example

An AI-retrosynthesis planner finding new chemical reaction chains

ACTING

Generating and controlling actions.

example

An AI assistant speaking to you

ASSESSING

Looking at the world.

example

Profile-building for search recommendations

INFERRING

Drawing conclusions.

example

A search engine suggesting 'remedies' when you search 'symptoms'

PREDICTING

Making guesses about what happens next.

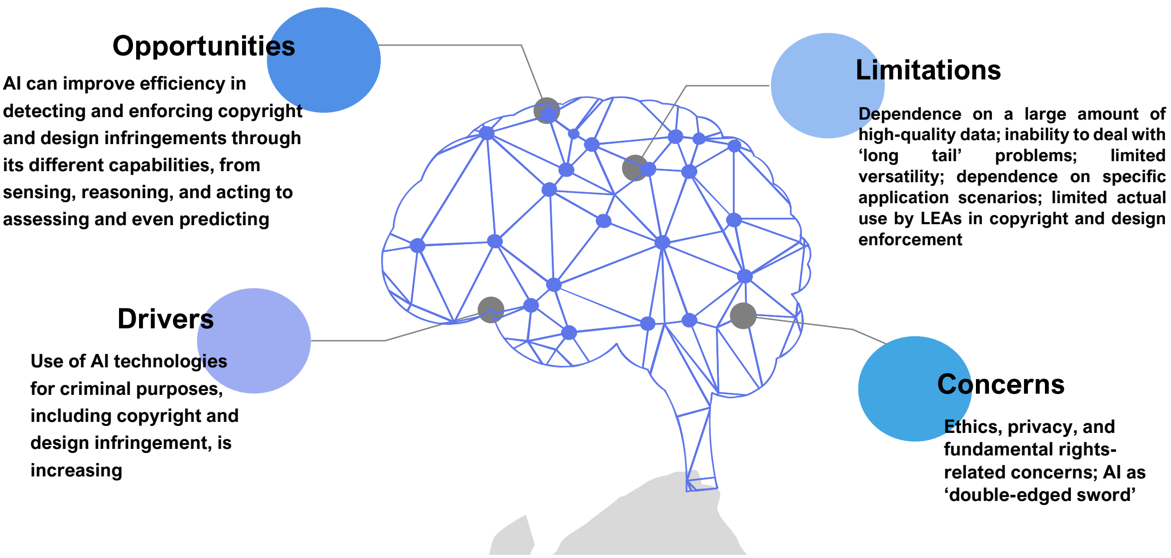
example

Deep neural networks predicting COVID-19's protein structure

AI has various subfields, each of which has its own specific aspects in addition to certain shared elements. These subfields pursue a number of operational objectives, including machine learning, natural language processing, computer vision, computer speech and expert systems. Quantum computing, although it is not necessarily linked to AI, could be used to enhance the capacity of AI applications, while explainable AI, encompassing a set of processes and methods, enables users to understand and trust the results generated by ML algorithms.

Against this background, the study found that there are multiple **opportunities**, **drivers**, **limitations** and **concerns** regarding the use of AI in infringement and enforcement of copyright and designs.

AI and copyright & design infringement and enforcement



Opportunities

AI can improve efficiency in detecting and enforcing copyright and design infringements through its different capabilities, from sensing, reasoning, and acting to assessing and even predicting

Limitations

Dependence on a large amount of high-quality data; inability to deal with 'long tail' problems; limited versatility; dependence on specific application scenarios; limited actual use by LEAs in copyright and design enforcement

Drivers

Use of AI technologies for criminal purposes, including copyright and design infringement, is increasing

Concerns

Ethics, privacy, and fundamental rights-related concerns; AI as 'double-edged sword'

There are several **opportunities** for AI to improve efficiency in detecting copyright and design infringements and in enforcing copyright and design rights, since it can be used to perform a number of different functions ranging from sensing, reasoning and acting to assessing and even predicting. Currently, the main areas of AI development are machine learning, natural language processing, computer vision, expert systems, and explainable AI. Explainable AI is currently receiving increased attention by experts and policy makers. Other technologies enhanced by AI, such as quantum computing, blockchain, 3D printing, generative design, cloud services, and robotics also have great potential. AI can identify and prioritise risks, instantly spot malware on a network, guide incident response, and detect intrusions before they occur. For example, machine learning stands out as a key AI subfield that can be used to develop law enforcement tools such as the analysis of large amounts of information to detect threats and identify social engineering bots, scanning of images to detect false pages or illicit content, improving automatic content recognition (ACR) tools, and providing insights to find infringement patterns.

Natural language processing can be used to analyse and block cyberattacks like phishing, identify the behaviour of fraudsters, and create a correlation analysis aimed at promptly identifying infringements. Computer speech and computer vision are also successfully employed in this field. Some of their uses include pattern recognition to predict future infringements, detection of marketing of infringing goods, and the detection and analysis of fraudulent logos or other images. Quantum computing could be adopted to improve AI tools, enabling them to process larger amounts of data. For example, AI and quantum computing can be used by customs and law enforcement authorities to recognise patterns within large datasets and identify similarities. Expert systems, on the other hand, can be used by law enforcement to decide which strategy is more adequate to protect a system from specific vulnerabilities, including those linked to copyright and design infringements.

As for the **drivers**, the various capabilities of AI make it attractive for malicious actors. AI can emulate many acts performed by humans and in some instances can exceed human performance in terms of efficiency and scalability. Moreover, certain crimes – with the support of AI technologies – can be performed on a much larger scale, targeting thousands of victims simultaneously. As depicted by the double-edged sword metaphor, the same technologies can be used both by malicious actors and for enforcement purposes, including in the field of copyright and designs. Fraudsters and criminal groups employ or may employ the same AI techniques used by enforcement agencies to overcome cybersecurity measures and evade detection. This is known as the 'AI/cybersecurity conundrum': as AI matures and is increasingly used in the field of cybersecurity, the potential downsides of this technological advance increase as well. In this regard, adversarial machine learning could help to spot and to overcome cybersecurity measures, including breaking through defences and developing dynamic malware to evade detection. AI technologies can be used to make such attacks more efficient, as in the case of AI-supported password guessing and CAPTCHA breaking. Furthermore, natural language processing tools can be employed to produce deepfake music videos, and generative design-based tools can be used in the manufacture of infringing copies.

Finally, it is worth keeping in mind that there is always a human being behind any AI algorithm and its practical application vectors. Explainable AI, though it does not solve all possible issues, could be used by law enforcement authorities as part of an increased use of innovative tools – including AI – in analysis and prediction, while at the same time better achieving the prerequisites of fairness, accountability and transparency. The use of AI in law enforcement and the judiciary should in any case always be subject to strong safeguards and human oversight through built-in human control.

The current **limitations** of AI include, in particular: its dependence on a large amount of high-quality training data; its inability to deal with long-tail problems (i.e. the difficulty and cost required for AI to achieve strong performance at the 'long tail' of data distribution); its limited versatility; its dependence on specific application scenarios; and the inherent biases of the AI's developer. More powerful machine learning algorithms can learn complex non-linear relationships between input and output data, but to do so they require a large amount of quality data. Machines still need to understand the world through perceptual and cognitive learning in a more accurate manner, enabling them to simulate real-world scenarios through reinforcement learning to perceive information and then transform that perceived information into abstract knowledge through attention, memory, and understanding. This might be achieved through the intersection, integration, and optimisation of algorithms and the continuous improvement of academic study. In addition, notwithstanding the expanded use of innovation technologies in law enforcement, according to the interviews undertaken in the context of this study the actual use of these technologies by public authorities to enforce copyright and designs is still generally limited. Furthermore, law enforcement and customs authorities will need to continuously monitor the new technology landscape to ensure they are properly prepared and trained.

Finally, the development and application of AI has raised some **concerns** related to ethics, privacy and fundamental rights. As AI and related technologies are used to make determinations and predictions in areas of great importance such as combating criminality, including copyright and design-related crime, AI has the potential to impact fundamental human rights in profound ways. AI algorithms are powered by data collected and processed by technologies that increasingly surround us at every minute of our lives.

Many experts argue that AI algorithms must be built to align with overarching human goals. The EU Parliament, in its recent Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)), has clearly stated that 'AI should not be seen as an end in itself, but as a tool, with the ultimate aim of increasing human well-being, human capabilities and safety'. As a result, the fundamental human right to privacy must be duly considered when data is collected by law enforcement authorities. Algorithms and AI should be 'ethical by design', with no built-in bias, in a way that guarantees maximum protection of fundamental rights. The EU Parliament in the same resolution invites 'European stakeholders, including the Member States and the Commission, to ensure, through international cooperation, the engagement of partners outside the EU in order to raise standards at international level and to find a common and complementary legal and ethical framework for the use of AI'. Policy makers are invited to be actively involved and to draw the legal boundaries within which these technologies are allowed to operate.

Retroactive deconstruction of an algorithm may be required to assess the factors that influence a model’s predictions.