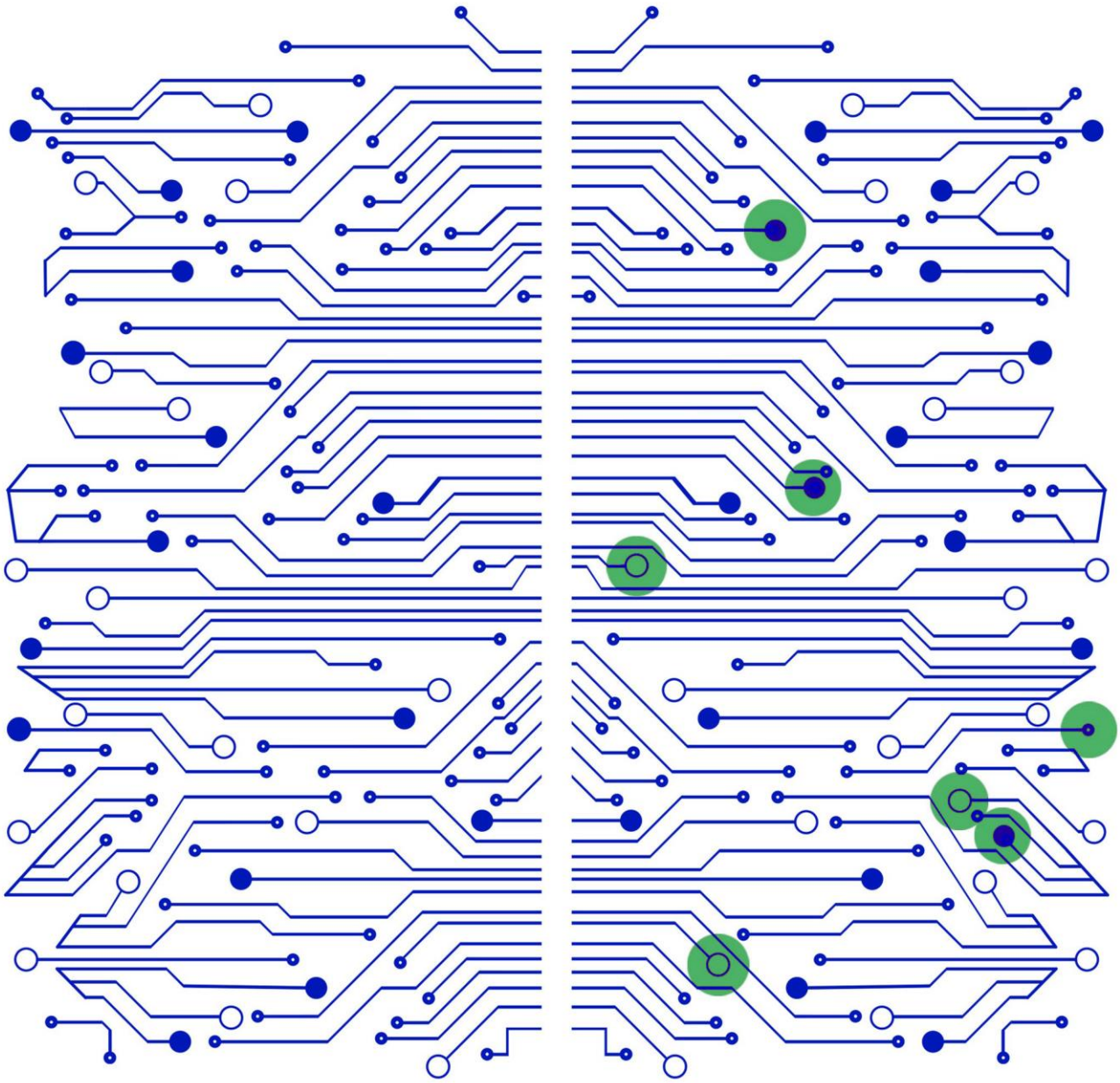
EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

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



September 2022

DISCLAIMER

The views expressed in this discussion paper do not represent any official position of the EUIPO. This paper is based on initial research by the Observatory, which was complemented by contributions from individual experts, including from the Observatory's expert groups on 'The Impact of Technology' and 'Cooperation with Intermediaries'.

Existing services or solutions provided by specific companies mentioned in this discussion paper are only intended as concrete examples of the implementation of automated content recognition technologies. Any reference to these services, solutions or companies can in no way be construed as a form of assessment or endorsement of the described service, solution or company.

The Observatory welcomes any further input or comments on this discussion paper in order to continue to develop its understanding of automated content recognition technologies and their potential implications for intellectual property. This discussion paper may be subject to reviews or updates, based on any further input from experts or new developments in the field.

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

ISBN 978-92-9156-326-5 DOI 10.2814/952694 TB-07-22-884-EN-N

Table of Contents

Executive Summary

The central role played by a number of automated content recognition (ACR) solutions in the development of innovative services drives major evolutions in this field of technology. The first phase of the analysis of these technologies ([1]) provided an overview of existing ACR technologies, how they are currently used and how they may develop in the future. It showed that different ACR technologies are used for a very broad range of purposes, going far beyond the protection or management of intellectual property (IP) rights.

This second phase of the analysis focuses on the uses of ACR technologies, and their potential as one of the tools that can support the protection and management of IP rights, through a series of concrete use cases.

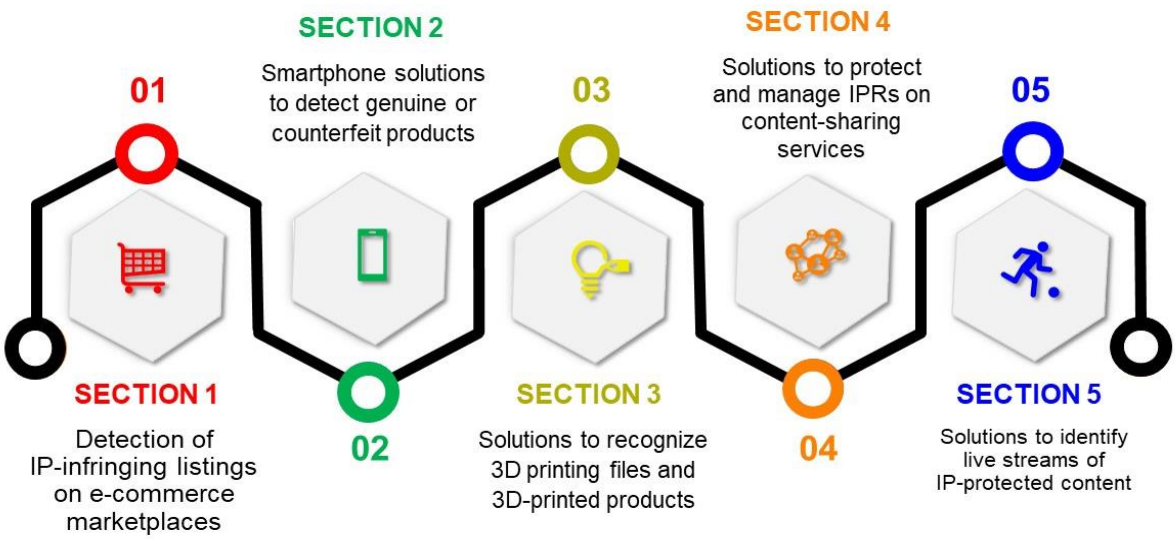


Figure 1: List of use cases – Source EUIPO

The use cases show that ACR technologies such as watermarking, fingerprinting or artificial intelligence (AI)-based solutions already support the IP enforcement activities of right holders and online intermediaries in relation to both physical products and digital content.

([1]) Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020.

- The use case on the **detection of IP-infringing listings in e-commerce marketplaces** describes how technologies such as logo, character or object recognition and image fingerprinting are deployed by some e-commerce marketplaces or third-party vendors for that purpose. It explains how the insight gained through ACR technologies can be combined with contextual information (e.g. keywords normally associated with IP-infringing listings) and behavioural data (e.g. sellers' history) to enhance the detection of IP-infringing listings and defeat new strategies by IP-infringers to escape detection. In this respect, it shows how ACR technologies are a component of broader solutions to deal with IP-infringing listings, which may include automated removal, notification or human review of listings to confirm their IP-infringing nature.

- The use case for **solutions to identify live streams of IP-protected content** describes how different ACR technologies can contribute to addressing the problem of illegal live streams at different levels.

    - **Forensic watermarking** involves embedding invisible information in the legal feed of live content. This can help to identify the source of leaked content appearing on piracy sites or IPTV services. This information is typically used by investigative teams to devise the most appropriate strategies to block future piracy activities.

    - **Fingerprinting** allows an extract of a piece of content to be recognised. IP owners and/or legitimate streaming services can use this to take more immediate action by identifying illegal live streams and getting them suspended. When deployed on legitimate streaming platforms, this requires cooperation with IP owners for partial fingerprints of the live event to be created in a matter of seconds before pirate streams start to appear. When deployed by third-party vendors monitoring illegal live streams on piracy sites or IPTV services, this requires close cooperation with the relevant intermediaries' services used by illegal streamers to streamline notice and action processes and achieve near-instant take down.

    - **AI-based solutions** recognise a type of event that is typically protected by IP (e.g. a football match), as opposed to a specific event. This new approach is combined with

the analysis of a set of signals to trigger and prioritise a human review to determine whether a stream is licit.

The use cases also explore the potential of ACR technologies to address some of the existing challenges faced by law enforcement authorities (LEAs), but also new challenges in protecting innovative production processes.

- The use case for **smartphone solutions to detect genuine or counterfeit products** explores the potential for using smartphones as a powerful technological platform to implement ACR technologies. It explains how this could deliver portable tools for LEAs to detect genuine and counterfeit products when performing searches or on-site inspections. Although these integrated solutions do not yet seem to be available to LEAs, a number of companies are developing ACR-based authentication solutions for smartphones, with applications to capture an image of a product that needs to be authenticated. The application can then use AI-based content recognition to analyse one or several specific features of the product (e.g. its pattern, trade mark or design) and determine whether it is genuine or counterfeit. Developing integrated solutions that would effectively serve the purpose of LEAs is likely to require the use of a specific AI-based content recognition solution that could be fed with information from a broad set of IP owners to detect potentially IP-infringing products.

- The use case for **solutions to recognise 3D printing files and 3D-printed products** explores the potential of watermarking solutions to trace the origin of a 3D model from its digital to its printed version. In this context, watermarking can be applied to the following.

    - **Individual 3D files:** this consists of embedding unique information directly into the individual copies of a 3D file before sharing it with an authorised user. Such watermarking solutions already exist and are typically used to identify the source of the illegal distribution of a specific 3D file.

    - **Printed objects:** this consists of embedding a visible or invisible watermark in a specific area or even into the surface of the object. Although there has been some research in this field, including on watermarks imperceptible to the human eye, these kinds of solutions are still under development and are not currently commercially available.

Finally, the use cases explore how ACR technologies can support the protection and the management of IP rights.

- The use case for **solutions to protect and manage IPRs on content-sharing services** explains how fingerprinting-based solutions, among others, can be used to identify specific copyright-protected content for which right holders have provided relevant and necessary information to online content-sharing service providers. Beyond describing existing solutions that have already been covered in other studies, this use case explores how ACR solutions can support copyright management and the assessment of legitimate uses of a copyright-protected piece of content with:

    - **parameters and rules for fingerprinting-based solutions** that can already be used to manage multiple rights on a single piece of content or allow a certain degree of tolerance in the use of copyright-protected content;

    - **AI-based ACR technologies**, such as logo, facial, text or speech recognition, that could be used in the future to analyse the context in which a specific piece of content or an extract from it is used, and to support human reviewers' assessment of the application of copyright exceptions or limitations.

For each use case, the discussion paper covers the advantages and the limitations of the different ACR technologies analysed, not only from a technical point of view, but also to address complex legal situations requiring a careful balance of potentially conflicting rights.

It is clear from this second discussion paper that ACR technologies continue to develop, and still have further potential to support the protection and management of IP rights. In this context, the Observatory will continue to closely monitor the development of new solutions in this field of technology.

Introduction

The central role played by a number of automated content recognition (ACR) solutions in the development of innovative services drives major evolutions in this field of technology. The first phase of the analysis of these technologies ([2]) provided an overview of existing ACR technologies, how they are currently used and how they may develop in the future. It showed that different ACR technologies are used for a very broad range of purposes, going far beyond the protection or management of intellectual property (IP) rights.

The various ACR technologies each have their advantages and limitations and support the recognition of content at different levels:

- **hashing** supports the recognition of digital files;
- **watermarking** supports the recognition of previously marked digital copies;
- **fingerprinting** supports the recognition of an extract of a piece of content; and
- **AI-based or enhanced solutions** support the recognition of specific features or elements of a piece of content, including the analysis of images of physical products ([3]).

In some cases, these technologies are combined to optimise the resources needed to recognise content while improving recognition. The greatest challenge in the development and deployment of any given ACR solution lies in striking the right balance between its accuracy in recognising content, its robustness in resisting content alteration, and the technical resources and investments needed to implement and operate it ([4]).

This second phase of the analysis focuses on the uses of ACR technologies and their potential as one of the tools that can support the protection and management of IP rights. Five use cases have been selected:

([2]) Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020.
([3]) Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020, p. 21 defines AI-based or enhanced solutions.
([4]) Including investment from individuals or companies that want their content to be recognised.

- solutions to detect IP-infringing listings on e-commerce marketplaces;
- smartphone solutions to detect genuine or counterfeit products;
- solutions to recognise 3D printing files and 3D-printed products;
- solutions to protect and manage copyright and neighbouring rights on content-sharing services;
- solutions to identify live streams of IP-protected content.

The objective of these use cases is to further explore how ACR technologies can be one of the tools to:

- support IP right protection and management for both physical products and digital content;
- support IP enforcement activities by right holders, intermediaries and law enforcement authorities;
- address existing and forthcoming challenges in enforcing and managing IP rights (e.g. 3D printing).

For each use case, the analysis consists of a description of:

- the challenges that ACR solutions can address on their own or in combination with other measures, and the different ways the relevant ACR technologies can be implemented by different players, referring to existing services and solutions ([5]);

- the advantages, limitations and potential of the ACR solutions identified, not only from a technical point of view, but also to address complex legal situations requiring a careful balance of potentially conflicting rights ([6]).

The end goal is to further understanding of what ACR technologies can deliver, but also of their limitations as one of the tools in supporting the effective enforcement or management of IP rights.

([5]) Existing services or solutions provided by a specific company are only included in this discussion paper to provide concrete examples of the implementation of ACR technologies. Any reference to these services, solutions or companies can in no way be construed as a form of assessment or endorsement of the analysed service, solution or company.

([6]) It is important to note that the challenges, advantages and limitations of the same ACR technologies may differ from one use case to another.

1 Detection of IP-infringing listings on e-commerce marketplaces

1.1 Challenges

The upward trend in online sales continues, with estimates of e-commerce accounting for up to 16.3 % of total retail sales in the EU in 2020 ([7]). It has been estimated that around 68 % of EU internet users shopped online during 2020 ([8]). There are multiple e-commerce channels, with EU data showing that 40 % of EU enterprises selling online used an e-commerce marketplace and 88 % of them used their own website ([9]).

New channels create new opportunities as well as new challenges. As e-commerce keeps growing, so does the focus of IP owners' strategies on protecting and enforcing their rights online. A MarkMonitor survey on 'The future of online brand protection' ([10]) found that, in 2018, 79 % of the brands surveyed had an online brand protection strategy in place (a 15 % increase over 2017) with 46 % of respondents citing the need to keep customers safe as their primary business objective.

Some e-commerce marketplaces are developing mechanisms and tools such as Notice and Action (N&A) mechanisms to prevent the misuse of their services to sell counterfeits, allowing IP owners to notify listings infringing their rights through various forms that can be completed and submitted online. Some marketplaces are also developing 'IP protection programmes' ([11]) to cooperate with IP owners and put in place preventive measures. This cooperation takes various forms, including giving IP owners access to a dedicated notification system facilitating the identification and removal of IP-

([7]) Statista, 'Retail e-commerce sales as share of retail trade in selected European countries from 2014 to 2019, with a forecast for 2020 and 2021', November 2020.
([8]) Ecommerce News Germany, 'Key takeaways from E-commerce Region Report: Europe 2020', February 2021. See also the European Commission study on 'Digital Economy and Society Index (DESI) 2020 – Use of internet services'.
([9]) Eurostat E-Commerce statistics, December 2018.
([10]) Q4 2018 Global Survey – 'The future of online brand protection: Threats, trends and business impact', MarkMonitor.
([11]) This is for example the case with Alibaba ('IP protection platform'), Amazon ('Brand Registry'), Ebay ('Verified Rights Owners' programme (VeRO)), Allegro ('Rights Protection Cooperation Program'), and Meta ('Brand Rights Protection').

infringing listings and sellers ([12]). Information provided by IP owners, as well as the notices filed, can also be used to improve the technical measures to proactively detect IP-infringing listings in e-commerce marketplaces, so that they can be taken down and made to stay down ([13]).

At the same time, a number of third-party vendors have developed dedicated services to monitor e-commerce marketplace listings and identify those potentially infringing IP, complementing the set of tools available to rights holders.

1.2 ACR technologies and solutions in use

In this context, ACR solutions are developed and deployed by the following.

- **E-commerce marketplaces**, which are developing and implementing their own in-house solutions, including the use of ACR applied to the pictures of e-commerce listings. These ACR solutions are typically part of a broader set of tools used to identify IP-infringing listings on their services.

- **Third-party vendors**, which are developing solutions that entirely or partly rely on ACR to detect IP-infringing listings and are making their services available to IP owners.

In both cases, ACR technologies are typically used in the following ways.

- **In combination with other automated detection tools**, in particular the analysis of various signals (e.g. the use of certain keywords, price points, sellers' data or history) to identify potentially IP-infringing listings.

([12]) The EUIPO has been working with a number of e-commerce marketplaces to gather information on their IP protection tools to make it easier for users to take action and use the resources made available. See the EUIPO's webpage on 'Protecting your rights on e-commerce marketplaces'.

([13]) The cooperation between a number of e-commerce marketplaces and IP owners is also supported by initiatives such as the 'Memorandum of understanding on the sale of counterfeit goods on the internet' facilitated by the European Commission, or the EUIPO's Strategic Project on 'Enhancing IP protection on e-commerce marketplaces'.

- **As part of broader processes** that may entail human review or automated notification of the listings detected. Some third-party vendors provide dashboards allowing IP owners' representatives to keep track of the listings detected, and to decide whether to send a notification to the relevant marketplaces.

A range of ACR technologies can be used to **recognise different types of content**, including:

- **registered trade marks/logos** appearing on e-commerce listing pictures;
- **registered designs** that can be matched with e-commerce listing product pictures;
- **protected patterns** (e.g. specific fabric patterns);
- **copyright protected pictures** of genuine products;
- **pictures of products** that have already been identified as infringing IP.

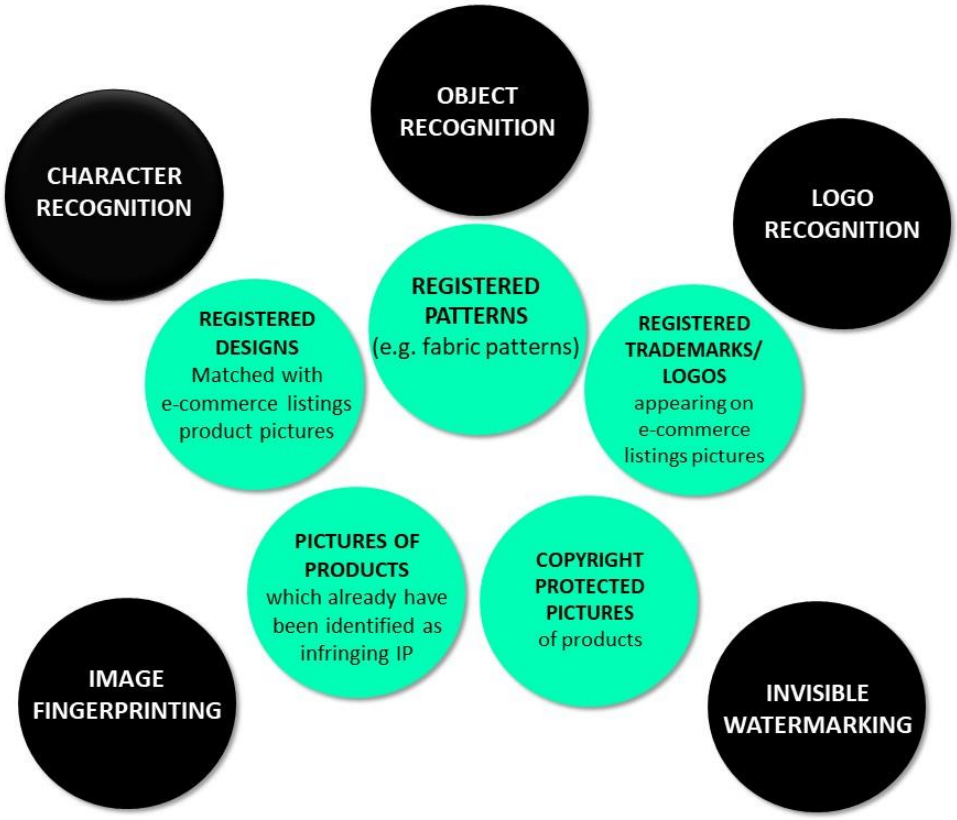


Figure 2: List of some ACR technologies with the types of content they can recognise – Source EUIPO

1.2.1 Types of technologies

Logo recognition is a specific category of image recognition(14) that can be used to detect the presence of trade mark-protected logos appearing on product pictures. It can contribute to identify potential counterfeits or products that should not feature the logo (e.g. a phone case displaying a renowned trade mark logo from a company that does not produce phone cases).

A logo recognition system can locate and identify a particular logo on a product picture, based on a collection of pictures the system has been trained with. It can also search within specific areas of a picture, based on where the logo should feature on the product. It is critical for any logo recognition solution to have a robust variable training set where logos appear in different positions and quality, as IP infringers often try to use distorted or blurred logos to escape detection. Advanced logo recognition technologies go beyond simple image matching, and use machine learning to identify a logo under different angles, or if it has been distorted(15). Some technologies are also able to detect a logo that has been adjusted, obscured or partly obfuscated(16). The accuracy of the solution depends on how it has been trained, but may vary depending on the specific characteristics of a given logo.

Character recognition allows the extraction of the text present in an image or document. It can be applied to pictures appearing in e-commerce listings to detect registered text trade marks. Most recent technologies use machine learning to increase automation, instantly read and process almost any type of image and accurately extract text appearing in it.

In some instances, IP infringers try to thwart automated detection of specific keywords in the text of their listings by embedding the trade mark name and/or product description into the product picture. Character recognition is used to overcome these kinds of strategies by detecting and extracting any text from the product picture. The text can be extracted from the product picture regardless of its resolution(17). Some third-party vendors have developed functionalities that allow search based on

(14) Image recognition is a general term applied to all image-based identifying technologies. See Red Points blog.
(15) See, for example, Incopro website.
(16) See Visua website (formerly LogoGrab) and Red Points blog.
(17) See Incopro website, BrandShield website and Smart Protection website.

the texts extracted from e-commerce product pictures to facilitate the identification of potentially IP-infringing listings.

Object recognition is a process that can identify an object or product in a picture. It can identify shapes, dimensions, and other elements of a specific object in real time through image processing ([18]). It can be used to detect products with registered design or protected patterns, for example specific fabric patterns. The use of machine learning facilitates multi-dimensional image comparison and analysis of product features such as labels, zippers, patterns and the texture of the material, as well as the collocation of these features on the product – going beyond a mere two-dimensional image comparison.

Products infringing a registered design do not necessarily reproduce the trade mark of the authentic product, making it more difficult to detect them through logo and/or character recognition. Some object recognition systems, trained with listings from relevant product categories with specific keywords, are able to identify and analyse product pictures and assign them a 'likelihood indicator', matching them with the image of a protected product or design. The higher the score, the more likely it is that the image contains the protected product or design ([19]). The accuracy of the solution depends on how the system has been trained to identify certain objects and may vary depending on the specific characteristics of a given product or registered design.

Image fingerprinting ([20]) can be used to identify copyright-protected pictures of products. It is an effective solution to protect 'brand-affiliated pictures' online, especially in situations where trade mark rights cannot be used as a basis for enforcement, as the picture itself does not display the protected trade mark (or it has been blurred or obfuscated). It can also be used to recognise pictures of products that have already been identified as infringing IP, and provide an effective solution to identify all the listings using identical or similar pictures, or make sure that new listings using the same picture effectively stay down.

([18]) See 'Understanding Computer Vision: how AI sees our world', 2020. See also Red Points blog.
([19]) See Red Points website.
([20]) See also Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020, p. 15-16.

These solutions analyse the visual information of an image, such as the dimension, colours, and spatial characteristics. This information is extracted and converted into a unique code (fingerprint) that is stored in a reference database of:

- copyright-protected pictures of products; and/or
- pictures of products previously identified as infringing an IP right.

Any image appearing in an e-commerce listing can be analysed against the fingerprints stored in the reference database; identical or similar images can be recognised even if they have been rescaled, reoriented or distorted, or if their brightness has changed.

Invisible watermarking can also be used to identify brand-affiliated pictures. The hidden 'watermark' can be detected and support the identification of a listing for a counterfeit product since the unauthorised use of a watermarked product picture may be a signal that the e-commerce listing may be for a counterfeit product ([21]). However, there are several techniques and tools available to circumvent watermark protection of images ([22]).

1.2.2 Types of ACR solution developers

In the context of this use case, ACR solutions are developed in-house by some e-commerce marketplaces or by third-party vendors offering brand protection solutions for IP owners.

E-commerce marketplaces developing in-house IP protection solutions, including ACR technologies, can use their own information resources, as well as the information provided by IP owners ([23]), to create large datasets for developing and training their ACR solutions, including:

- **logo, character and image recognition solutions**, the accuracy of which depends on large databases of pictures that are used to train these solutions;

([21]) See IMATAG and Digimarc websites on invisible watermarking.

([22]) See Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020, p. 14.

([23]) E-commerce marketplaces use information provided through notifications of IP-infringing listings and in some instances through specific programmes specifically designed to gather information from IP owners.

- **fingerprinting solutions**, the effectiveness of which depends on the fingerprints of pictures that have been included in the reference database.

In both cases, access to large datasets of e-commerce listings and pictures provided by IP owners contribute to the effectiveness of the ACR solutions deployed. Some e-commerce marketplaces have set up IP protection programmes to collaborate with IP owners, including on the gathering of data and pictures that can improve their ACR solutions.

This is the case for example for Amazon and its Brand Registry ([24]), which, among other information, allows IP owners to share product pictures, brand logo(s), packaging images, and online presence information such as websites and social media pages ([25]). This is also the case for Meta's Brand Rights Protection, which, among other tools supporting IP right protection, allows rights holders to upload information about their trade marks, logos and product pictures.

Third-party vendors develop various brand protection solutions. The detection processes behind these solutions are performed by tools scanning the listings of e-commerce marketplaces. For example, Red Points ([26]) uses detection bots that scan through e-commerce marketplaces, making use of different ACR solutions to identify listings that may infringe pre-identified IP rights. If it identifies such a listing, it can automatically notify it directly to the marketplace or do so only after validation by the IP owner.

Depending on the third-party vendor, the detection processes may involve logo recognition, character recognition, object recognition, image fingerprinting or invisible watermarking, or a combination of all or some of these technologies. A number of companies are working on such solutions, such as VISUA ([27]), Smart Protection ([28]), SGS ([29]), and Nanomatrix ([30]), combining AI-based technologies to monitor and identify IP-infringing listings on e-commerce marketplaces and other

([24]) Amazon Brand Registry. Brand owners enrolling in Amazon's Brand Registry are required to provide information about their registered text trade marks and logos. Once Amazon has verified the information submitted during enrolment, registrants are given full access to Brand Registry's tools to help sellers protect their brand.
([25]) See Amazon's Brand Registry FAQ.
([26]) See Red Points website.
([27]) See VISUA website.
([28]) See Smart Protection website.
([29]) See SGS website.
([30]) See Nanomatrix website.

online services such as social media platforms. Incopro[31] uses logo recognition and character recognition in its brand protection solution. Brandshield[32] also develops character recognition technology, image fingerprinting and object recognition technologies as part of its brand protection solution.

Similar to the solutions deployed directly by e-commerce marketplaces, ACR technologies are used in combination with other automated detection tools supporting the analysis of context information (e.g. keywords or price) to identify potentially IP-infringing listings.

1.3 ACR's potentials and limitations

The potentials and limitations of the ACR technologies used may differ depending on whether the solution is implemented by an e-commerce marketplace or by a third-party vendor.

- **Improvement of IP protection through content recognition**: AI-based or -enhanced content recognition solutions can improve the detection of pictures of IP-infringing products in e-commerce listings. The combined use of logo, character and object recognition can improve the level of recognition and detect protected logos and text trade marks even if the logo or the picture have been distorted. Advanced technologies can also support the detection of design replicas solely based on the shape of the product.

- **Data resources**: AI-based recognition solutions require significant data storage and computational resources[33], as well as access to relevant datasets. They also require a considerable amount of work by highly skilled technical professionals[34], which is why IP owners typically rely on solutions developed by third-party vendors. To develop, train and implement AI-based or enhanced recognition technologies, both e-commerce marketplaces and third-party vendors require a significant quantity of images, descriptions and other

[31] See Incopro website.
[32] See BrandShield website. See also BrandShield's company announcement, January 2021.
[33] See Mike Bernico, The Data Question, *Towards data science*, December 2018. See also Chen Sun, Abhinav Shrivastava, Saurabh Singh, and Abhinav Gupta, Revisiting Unreasonable Effectiveness of Data in Deep Learning Era, August 2017.
[34] See WebFX, AI Pricing: How Much Does Artificial Intelligence Cost?, 2021.

metadata related to the products. Even more data is required to train deep learning models ([35]).

- **Accuracy**: the accuracy of AI-based or enhanced content recognition solutions largely depends on the amount and quality of data provided to train the systems, but also on the product and related IP right that is to be recognised: the more generic the shape and form of the product, logo or design, the more difficult it is to avoid false positives or negatives. In complex cases, where there are only a number of similarities between two images, determining the level of accuracy of a given solution can also be a challenge, as the identification of relevant similarities may depend on the perception of individuals, which may differ.

  The recognition of 3D designs and trade marks also raises specific challenges, in particular with regard to designs protecting products, as the viewing angle on the product pictures of a listing may not correspond to any of the protected design pictures. However, with the use of machine learning, AI-based or -enhanced recognition technology can constantly acquire more data to learn from, providing more accurate results.

- **Combined use with other technologies**: AI-based or enhanced content recognition technologies can be used in conjunction with other ACR solutions such as the fingerprinting of copyright-protected pictures or character recognition. The insight gained through ACR technologies can also be combined with context information (e.g. keywords normally associated with IP-infringing listings or prices) and behavioural data (e.g. sellers' history, sudden increases in reviews, or sources of the traffic to a given listing ([36])) to support the detection of potentially IP-infringing listings, which can trigger an automated suspension or removal and/or a human review.

- **Other factors**: although ACR solutions already help to identify a number of blatantly IP-infringing listings on e-commerce marketplaces, some of their limitations are not linked to the technologies themselves, but to the complexity of determining what constitutes an IP infringement in specific cases. This is, for example, the case when an object recognition

([35]) InData Labs, 'Deep Learning in Image Recognition Opens Up New Business Avenues' (July 2019).
([36]) For example, traffic from a website dedicated to the promotion of IP-infringing products.

solution identifies a picture of a product that merely resembles a registered design, or when a logo recognition solution identifies a logo that is used as a parody. This makes human review necessary in situations where an ACR solution identifies products that are similar but not identical, or where a legal assessment is needed to balance conflicting rights.

2 Smartphone solutions to detect genuine or counterfeit products

2.1 Challenges

'(I)n 2019, imports of counterfeit and pirated products into the EU amounted to as much as EUR 119 billion …, which represents up to 5.8 % of EU imports'([37]). In this context, EU customs authorities are at the forefront of detecting counterfeit products. The growing number of imported genuine and counterfeit products raises new challenges and underlines the importance of close cooperation and information exchange between law enforcement authorities (LEAs) and IP owners as key to improving IPR enforcement and identifying IP-infringing products ([38]).

This also requires continuous effort to monitor the trade in counterfeit products and technological solutions to improve risk assessment and identification of such products ([39]).

Technological solutions are already being developed to support these objectives, such as the establishment of common databases and platforms for sharing data on genuine and counterfeit products ([40]).

However, in many instances LEAs need portable tools and solutions to authenticate products when performing searches or on-site inspections, and smartphone devices provide a powerful technological platform to support the development of ACR-based solutions in that field ([41]). Although these solutions do not currently seem to exist for LEAs, some examples from companies developing

([37]) EUIPO/OECD, Global Trade in Fakes, 2021, p. 8.

([38]) See the Directorate-General for Taxation and Customs Union's website.

([39]) 'Trends in Trade in Counterfeit and Pirated Goods', 2019, p. 35; 'Report on the EU customs enforcement of intellectual property rights – Results at the EU border 2019 (2020)'. See also 'Misuse of Small Parcels for Trade in Counterfeit Goods' (2018). The majority of articles detained by customs are suspected of infringing trade mark rights, but design and patent infringements have become more common, as have copyright infringements.

([40]) In 2019, the EUIPO has consolidated its different enforcement tools under one portal, the IP Enforcement Portal (IPEP). See also 'Status Report on IPR Infringements', June 2020.

([41]) See Gianmarco Baldini, Eduardo Cano Pons, 'Enforcers and brand owners' empowerment in the fight against counterfeiting', JRC Technical Report (European Commission, 2017) p. 12.

ACR solutions for smartphones illustrate the potential for these technologies to help LEAs, resellers, retailers, and end users authenticate genuine goods.

2.2 ACR technologies and technical solutions in use

This use case explores the different ACR technologies that can be deployed on smartphones to authenticate genuine goods – and by extension detect counterfeits – for three main purposes:

- **detection of counterfeit products by LEAs** through widely available smartphone devices that can be used remotely where checks are taking place;
- **detection of counterfeit products by retailers and resellers**, for example in the context of product returns or inventory verification;
- **identification of genuine products by final customers**, facilitating quick and easy verification of a product's authenticity.

A number of companies are developing ACR-based authentication solutions for smartphones, with applications to capture an image of a product that must be authenticated. The application can then use ACR to analyse one or several of the specific features of the product and determine whether it is genuine or counterfeit, including:

- **protected patterns**, for example a specific fabric pattern ([42]);
- **registered trade marks** appearing on the product ([43]);
- **registered designs** of the product ([44]).

Companies providing smartphone authentication solutions use various databases consisting of images of physical goods that they have collected by themselves or in collaboration with IP owners.

([42]) For example Entrupy's Luxury Authentication solution can recognise the materials and leathers of luxury branded handbags and accessories and score the item as either authentic or unverified based on the images of the product submitted.
([43]) Entrupy's Sneaker Authentication solution can extract and detect text elements from captured image of a sneaker.
([44]) Entrupy's solutions are able to detect the protected design of a handbag or a pair of sneakers.

These databases can be used to compare images of physical products or packages taken with a smartphone, or to train object recognition algorithms.

ACR-based solutions can be deployed in conjunction with or in addition to other existing technologies supporting authentication, such as track-and-trace tools, radio frequency identification (RFID), QR serialisation codes, near-field communication (NFC) or any other technology based on adding security elements to a product. Further information on these technologies can be found in the EUIPO's 2021 'Anti-Counterfeiting Technology Guide'([45]). They are not covered in this use case, as this discussion paper focuses on fingerprinting and AI-based or -enhanced content recognition solutions.

2.2.1 Smartphones and mobile ACR

Smartphone devices offer a powerful technological platform for the development and deployment of ACR solutions. These devices can be directly incorporated into the detection of counterfeit goods by customs authorities and/or the authentication of genuine products by consumers, as they are providing several key functionalities for these purposes([46]).

- **Capturing** recognisable features of a product such as its colours, shape, packaging and dimensions, as well as of its labels or other details, through high-resolution cameras. The latest generation of smartphone cameras also include 3D sensing technologies([47]) that augment camera capabilities for facial and object recognition and can capture the actual length, width and height of a physical product. Smartphones can also be connected to external plug-in devices such as spectrometers or microscope lenses, all adding other sets of recognisable features that can be captured.

([45]) See 'Anti-Counterfeiting Technology Guide' prepared by The European Observatory on Infringements of Intellectual Property Rights, EUIPO, with support from the Anti-Counterfeiting Technologies Expert Group and the Impact of Technology Expert Group (2021).
([46]) EU Commission JRC Technical Reports, 'Enforcers and brand owners' empowerment in the fight against counterfeiting', 2017.
([47]) See FutureBridge, '3D Sensing – New Ways of Sensing the Environment'.

- **Connecting** to mobile data networks and other devices. Smartphones can send and receive data to and from remote servers, supporting access to datasets and processing power that far exceed the device capacity. Smartphones also include an increasing number of communication standards supporting the connection with other technologies such as NFC, RFID, and global satellite navigation systems([48]).

- **Processing** of data locally or remotely. Smartphones' capacity to process data locally is constantly improving([49]). For example, modern smartphones are able to process and qualify video streams to select the frame that contains a fingerprint image of high quality or process data for fingerprint comparison with reference databases([50]). Smartphones also allow data processing on remote servers.

2.2.2 Types of technologies

Fingerprinting can enable the recognition of the unique surface characteristics of a product such as microscopic irregularities([51]). Some companies use fingerprinting solutions that exploit data provided by IP owners to generate a unique fingerprint of products and packaging. The generated fingerprints are stored in a reference database for comparison([52]). In some cases, IP owners can monitor all product verifications through a smartphone application, ensuring better communication between IP owners, LEAs, and customers. The following are examples of this.

- EDGYN([53]) has developed a solution allowing end consumers and LEAs to verify the authenticity of a product through a dedicated application by scanning the product package with their smartphones. The pictures of the product are fingerprinted and compared with

([48]) See 'Anti-Counterfeiting Technology Guide' prepared by The European Observatory on Infringements of Intellectual Property Rights, EUIPO, with support from the Anti-Counterfeiting Technologies Expert Group and the Impact of Technology Expert Group, 2021.
([49]) See Science Museum, 'A computer in your pocket: the rise of smartphones', 2018.
([50]) Jannis Priesnitz, Christian Rathgeb, Nicolas Buchmann, Christoph Busch, Marian Margraf, 'An overview of touchless 2D fingerpring recognition', *EURASIP Journal on Image and Video Processing*, February 2021.
([51]) For example EDGYN and AlpVision use fingerprinting technology in their product authentication technology, which is used with smartphones and a dedicated mobile application.
([52]) See also Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020, p. 15-16.
([53]) See EDGYN website on their mobile anti-counterfeiting solution ADFIRMIA.

reference fingerprints, and the application notifies the user whether the product is genuine or not. AlpVision ([54]) provides a similar authentication technology.

- Bosch ([55]) has developed a product authentication solution that generates a reference fingerprint from the picture of a designated area of a product's surface. End consumers can take a photo of the same designated area of the physical product using their smartphone, which is processed and compared with the reference fingerprints. In this application, IP owners receive a notification each time a consumer scans a product, which enables the product to be tracked through different distribution channels.

AI-based or -enhanced content recognition solutions allow the recognition of specific features or elements of a product. In particular, **object recognition** ([56]) can be used to identify a physical product by taking a picture with a smartphone to detect its textural features, such as fabric patterns, and/or its shape and design. The technology can recognise microscopic characteristics of a product that are invisible to the human eye. In order to detect these microscopic characteristics, the solution might require the use of external devices compatible with smartphones, such as handheld spectrometers, sensors or additional lenses ([57]). Unlike fingerprinting technology, which compares fingerprints of images with reference fingerprints, object recognition compares the optical characteristics of a product with the previously learned optical characteristics of a reference product. The following are some examples.

- Entrupy ([58]) has developed a smartphone application that requires **the use of an external physical lens** to capture high-resolution microscopic images of some of a product's features. The application allows users to submit images of some of the microscopic features of a product, which are analysed to automatically determine whether it is genuine or counterfeit.

([54]) See AlpVision webpage.

([55]) See Bosch's website on 'Secure Product Fingerprint'.

([56]) For example Entrupy and Origyn apply object recognition technologies to differentiate between the genuine versions of a product and counterfeit products.

([57]) See GoyaLab, GoSpectro handheld spectrometer; see also Entrupy website. Smartphones are also widely used as a means of capturing spectra looks across a broad range of scientific (e.g. biomedical, chemical and agricultural) application areas. See A. J.S. McGonigle, T. C. Wilkes, Tom D. Pering, Jon R. Willmott, Joseph M. Cook, Forrest M. Mims and Alfio V. Parisi, 'Smartphone Spectrometers' MDPI, 2018.

([58]) Entrupy website; see also an article in the *Wall Street Journal*, 'AI Is a New Weapon in the Battle Against Counterfeits', August 2020, and an article from the Association for Computing Machinery, 'The Fake vs Real Goods Problem: Microscopy and Machine Learning to the Rescue', August 2017.

For example, the leather's micro-structure of a product can be used to automatically determine whether it is genuine or counterfeit.

- IBM ([59]) has developed an AI-based external optical device to be connected to a smartphone, used to recognise the specific characteristics of a product and verify its authenticity.

- Origyn ([60]) has developed a mobile application allowing end customers to authenticate luxury watches using object recognition.

- Entrupy ([61]) has developed a solution for IP owners and other businesses to authenticate sneakers using object recognition. Using a dedicated smartphone application, the solution can detect genuine trainers from selected brands by analysing the captured images of the tags and other pictures of the trainer taken from different angles. The solution provides instant confirmation through the app whether the trainer is genuine or unidentified and therefore potentially fake.

2.3 ACR potentials and limitations

- **Improvement of IP protection through content recognition**: using smartphones in authentication solutions can be cost-effective and resource-efficient, as the results can be provided via a smartphone application in real time or within a short period. As ACR solutions are based on product characteristics, the need for specific security features can sometimes be reduced or eliminated.

  Moreover, the use of smartphone solutions does not require expensive training, which facilitates their use by LEAs, intermediaries, and end consumers. In addition, smartphone technologies are constantly evolving and expanding their abilities to capture and process

([59]) See IBM's website on Crypto Anchor Verifier. Their solution can be combined with blockchain to ensure that a product's origin and contents match the blockchain record.
([60]) See Origyn's webpage. Origyn allows luxury watch IP owners to create an exact digital copy of each watch by using a smartphone and an application. The digital copy is then registered in a database, which is used to authenticate the watch by end customers. For example, in the pre-owned market, a buyer of a watch can take a photograph of the watch using Origyn's application, and the application will then process the data and identify the watch.
([61]) See Entrupy's sneaker authentication webpage.

information, which allows ACR-based solutions deployed on smartphones to evolve simultaneously ([62]).

- **Data resources**: AI-based or enhanced content recognition solutions require a large amount of data to ensure a minimum level of accuracy. For the ACR technologies used in smartphone detection solutions to be able to process and compare all the data collected and received, the quality of the datasets plays a central role in the training and improving of the detection models. Feeding the datasets with captured images taken by smartphone users requires a lot of computational resources to collect, store and process the received data. Depending on the product and the complexity of the fingerprint, resources needed to generate, store, and verify them by comparing may vary greatly ([63]).

- **Accuracy**: ACR technologies used with existing smartphone technologies can offer a high level of accuracy, as they decrease the risks of false positives and false negatives. Using large datasets consisting of high-quality data can result in very high accuracy rates. Coupling the smartphone with external devices such as microscopic lenses can also improve the accuracy of the results by enhancing the quality of the captured images. The accuracy of ACR technical solutions may depend on the complexity of the generated fingerprint and on the capturing capabilities of the mobile device, as well as on the number of recognisable features that can be extracted from the captured image to generate the fingerprint and compare it to a reference fingerprint.

- **Combined use with other technologies**: ACR technologies can be used as an alternative or in conjunction with other technologies such as NFC, RFID, taggants, stickers, holograms or QR codes. The combined use of these technologies with AI-based ACR solutions and fingerprinting technologies can improve the effectiveness and accuracy of the solutions and make them more difficult to circumvent ([64]). ACR technologies can also be used in conjunction with technologies such as blockchain to control the supply chain and product distribution ([65]).

([62]) See for example an article on AIpVision's webpage.
([63]) See Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020, p. 20.
([64]) See for example Bosch's solution combining QR codes and fingerprinting to provide a comprehensive brand protection solution.
([65]) See for example IBM's Crypto Anchor Verifier.

- **Other factors**: although a number of ACR-based apps have been developed to support the identification of genuine products from specific brands, they have limited value for the detection of counterfeit products by LEAs, that cannot use a broad set of brand specific apps in the context of their control activities.

  There is an ongoing pilot for a mobile app by French LEAs, through which they can send pictures of potentially IP-infringing products to relevant IP owners, who will then determine whether the product does in fact infringe their rights. However, the piloted app does not use ACR([66]). Developing an ACR-based mobile app that would effectively serve the purpose of LEAs is likely to require a specific ACR solution that could be fed with information from a broad set of IP owners to detect potentially IP-infringing products.

([66]) See 'Innovation gendarmerie: une nouvelle application pour traquer les contrefaçon', April 2021 (French only).

3 Solutions to recognise 3D printing files and 3D-printed products

3.1 Challenges

The development of 3D printing supports a move away from mass production to more localised production. It results in modern manufacturing processes and business models based on on-demand production of generic (e.g. car parts) or highly personalised objects (e.g. body implants) ([67]). 3D printing consists of two main phases: the creation of the digital design of the object (the Computer-Aided Design (CAD) 3D printing file) ([68]), and its printing using a 3D printer. This process is also commonly referred to as additive manufacturing (AM) ([69]).

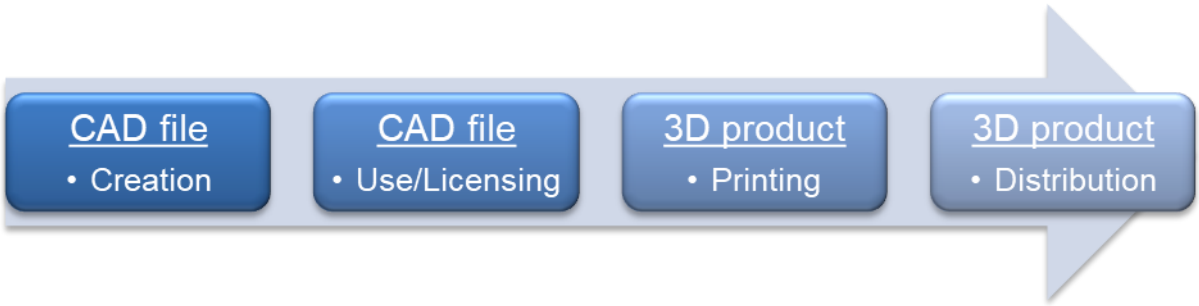


Figure 3: Different steps of the 3D printing process – Source EUIPO

There are three main business models in the 3D printing value chain ([70]):

- the commerce in Computer-Aided Design (CAD) files;
- the commerce in 3D printers;
- the commerce in printed products.

([67]) See the EPO's study 'Patents and additive manufacturing: Trends in 3D printing technologies', July 2020, p. 19. See also, for example, the Materialise website, which offers various types of 3D printing solutions and services.
([68]) In this analysis, the term 'CAD file' is used as a generic term for all file formats related to 3D printing.
([69]) WIPO Magazine, '3D printing and IP law', February 2017.
([70]) EUIPO study, 'IP infringement and Enforcement – Tech Watch Discussion Paper 2020', September 2020, p. 36.

From the creation of the CAD file to the printing of the object, a number of IP rights may be involved:

- the CAD file from which the printers execute instructions to create an object can be protected by copyright;
- the design of the printed object can be protected, whether it is registered or not;
- the design of the printed object may be eligible for copyright protection;
- the design features of the objects may also be protected by trade mark if the features are distinctive from the trade source ([71]);
- printing machines and the processes carried out by these printers, as well as functional printed objects (e.g. tools or mechanical components) can be protected by patents ([72]).

The European Commission noted that the absence of specific regulation of 3D printing and the lack of clarity on the scope of design rights in the digital environment, challenges its use in many key sectors. Its uptake also passes by clarifications on the protection of 3D printing files and on the application of the copyright private use exception to those files ([73]).

3D printing also enables the replication of almost any object, which can lead to new forms of product piracy and the manufacture and marketing of counterfeits. It also raises questions over the role and responsibility of 3D printer manufacturers and any other intermediary playing a role in the 3D printing value chain – from the creation and dissemination of the object design or CAD files to the actual production and dissemination of the-3D printed object ([74]). These aspects are not covered in this use case, which focuses on the use of ACR to recognise protected 3D printing files and related 3D-printed objects.

Just like any other digital files, CAD files can easily be shared and transferred, and a number of CAD files are openly and freely shared on the internet. With the growing number of individual users of 3D

([71]) Tesh W. Dagne & Chelsea Dubeau, '3D Printing and the Law: Are CAD Files Copyright-protected?', April 2020, p. 107-108. See also Workman Nydegger, 'IP Issues Resulting from 3D Printing', August 2017.

([72]) See EPO study, 'Patents and additive manufacturing: Trends in 3D printing technologies', p. 20, July 2020.

([73]) European Commission's IP Action Plan, 25 November 2020, p. 2; European Commission's study on 'The Intellectual Property Implications of the Development of Industrial 3D Printing', carried out by Bournemouth University', February 2020; see also IP Legislative Observatory of European Parliament resolution of 3 July 2018 on three-dimensional printing, a challenge in the fields of intellectual property rights and civil liability EP 2017/2007(INI).

([74]) Dr. Peter Schramm and Alessandro Burro: 3D printing and intellectual property: issues and solutions. INTA 11 February 2021.

printers, a number of companies in the field have created websites supporting the sharing of original CAD files for their customers to print their own objects ([75]). The terms and conditions of such websites typically request the CAD file creators to license all the rights required for its use ([76]), and some websites also support the licensing of CAD files under Creative Commons licences ([77]).

3.2 ACR technologies and technical solutions in use

Two key challenges for ACR in the field of 3D design are the design attribution and identification of 3D-printed products. This analysis focuses on **the use of watermarking technologies** to address these challenges and trace the origin of a 3D model from its digital version (CAD file) to its printed version ([78]). In this context, watermarking can be applied to the following.

- **Individual CAD files**, to identify the origin of a file that is illegally distributed ([79]).
- **The printed objects**, to identify IP-infringing 3D-printed objects that are offered for sale. Although the analysis focuses on watermarking that can be added directly to the object as part of the 3D printing process, the solutions typically used to protect manufactured products can also be applied to 3D-printed products ([80]).

3.2.1 Watermarking of the CAD file

Watermarking is typically used to identify the source of the illegal distribution of a CAD file. It consists of embedding unique information directly into the CAD file before sharing it with an authorised user (e.g. a 3D printing shop or manufacturer). This requires a software application, which is used to

([75]) Tesh W. Dagne & Chelsea Dubeau: '3D Printing and the Law: Are CAD Files Copyright-protected?', April 2020, p. 108.
([76]) A few examples of websites where users can easily download 3D printing file formats are: Cults, Free3D, GrabCAD, MyMiniFactory, Pinshape, and YouImagine.
([77]) Thingiverse and SketchFab allow CAD file owners to select a secondary copyright licence to determine how others may use the content. In this regard, the website suggests using one of the Creative Commons licences.
([78]) B. Macq, P. R. Akface, M. Montanola – 'Applicability of Watermarking for IPRs Protection in a 3D Printing Scenario', May 2017.
([79]) The use of watermarking does not give insight into how a CAD file was leaked, nor does it provide information on the channels through which it was distributed.
([80]) See, for example, the technologies presented in EUIPO's Anti-Counterfeiting Technology Guide, 2021.

embed unique information into the CAD file and protect it with a secret key. This secret key is needed to find out whether the file has been watermarked.

The identification process consists of uploading the watermarked CAD file to a dedicated platform and using the secret key to recover the information embedded in it. This way the owner of the IP rights on a watermarked CAD file who finds unauthorised copies of it can identify the source of the illegal distribution.

For example, Watermark3D ([81]) by Treatstock offers a solution to watermark a CAD file without any structural changes to the CAD project or visual marks to the final product. The creators of the CAD files can upload files in the provider's platform, embed watermarks into the files and acquire passwords to access them. The creator can then use the watermarks to detect the source of illegally distributed files. The technology is designed so that any attempt to remove the watermark would severely damage the 3D model.

3.2.2 Watermarking of 3D printed objects

Such solutions are still under development and not currently commercially available. Based on research papers, embedding a watermark on 3D printed products can be performed in a similar way as for CAD files ([82]). The visible or invisible watermark can be placed on a specific area of a printed product, or embedded into the surface of the product ([83]).

Researchers are exploring new methods to develop watermark algorithms for 3D printed products that resist alteration and other 'attacks'. Some researchers propose a solution for 3D mesh models, embedding watermarks into the functional part of a mesh file, which would be imperceptible to the

([81]) See Watermark3D website.

([82]) See Benoît Macq, Patrice Rondao Alface, Mireia Montanola, Applicability of watermarking for intellectual property rights protection in a 3D printing scenario, *Web3D '15: Proceedings of the 20th International Conference on 3D Web Technology*, June 2015, p. 89–95; See also Jong-Uk Hou, Dongkyu Kim, Won-Hyuk Ahn, and Heung-Kyu Lee, Copyright Protections of Digital Content in the Age of 3D Printer: Emerging Issues and Survey, IEEE Access, August 2018.

([83]) See EUIPO, Intellectual Property Infringement and Enforcement Tech Watch Discussion Paper, 2020, p. 35.

human eye and could resist various attacks([84]). The research into these solutions is advancing, and a number of patents have been filed in this field([85]).

Detecting and identifying the watermark on the product can be performed by a 3D scanning technology. In order to decode the watermark, the 3D object must be digitised via a scanning process reconstructing the surface model. Scanning can be performed by sensing the entire surface of the 3D product, or only parts of it, with dedicated scanning software([86]).

3.3 ACR potentials and limitations

- **Improvement of IP protection through content recognition**: watermarking offers solutions to trace and determine the authorship and/or ownership of CAD files using invisible watermarks that are almost impossible to detect and difficult to alter([87]). However, such solutions do not appear to be widely used, and some 3D printing file format may not have the necessary features to embed watermarks([88]).

  For watermarks embedded in 3D-printed objects, a number of studies suggest that this could be an effective way of embedding IP rights information, if it is possible to maintain the watermark unchanged during the object design and additive manufacturing. However, such technologies are still under development, and some researchers have suggested that other

([84]) Mesh is the structure of triangles or polygons that form the surface of the digital object. It is possible to modify the mesh by changing the size of these polygons. See, for example, studies from K. Wang, G. Lavoué. F. Denis, A. Baskurt, 'A Benchmark for 3D Mesh Watermarking', 2010; L. Jing, W. Yinghui, H. Wenjuan, L. Ye, 'A New Watermarking Method of 3D Mesh Model', 2014; O. M El Zein, N. I. Ghali, L. M. el Bakrawy, 'A Robust 3D Mesh Watermarking Algorithm utilizing Fuzzy C-Means Clustering', 2017; M. Narendra, K. T. Vaila, K. Nandhini, 'Invisible Watermarking in 3D models', 2018.

([85]) See, for example, the article by Sam Davies from tct Magazine (December 2020). The method includes an algorithm that adds a watermark to the product that remains almost invisible to the human eye, and is unlikely to be lost during the design and additive manufacture of the part. It enables the tracing of item-level information, including the 3D printing platform used and the individual responsible for the design.

([86]) B. Macq, P. R. Akface, M. Montanola 'Applicability of watermarking for intellectual property rights protection in a 3D printing scenario', May 2017. See also Yamazaki et al. 'Extracting Watermark from 3D Prints', 2014.

([87]) European Commission, 'The Intellectual Property implications of the development of industrial 3D printing', February 2020, p. 173.

([88]) European Commission's study on 'The Intellectual Property implications of the development of industrial 3D printing', carried out by Bournemouth University, February 2020.

technologies could be more effective for companies to protect their IP on printed objects, such as RFID tags or serial numbers ([89]).

- **Data and computational resources**: recognising previously watermarked CAD files does not require significant data or computational resources, especially since there is no need for a reference database. However, using an ACR watermark software to insert individual watermarks into every single copy of a CAD file or printed product and to detect them again can require significant resources. In addition, in the absence of generic or standardised watermarking technologies, a watermark generated by one technology cannot be read by a system using a different technology ([90]).

- **Accuracy**: digital watermarking technology can offer a high level of accuracy when tracing the source of a CAD file. However, these watermarks can be altered or removed, in particular by 'remeshing' the entire geometry of the polygons of the 3D object ([91]).

- **Combined use with other technologies**: Although watermarking can be used in conjunction with other technologies, this does not currently appear to be common practice when watermarking CAD files. When it comes to the recognition of 3D-printed products, some 3D scanner mobile apps already exist, making use of photogrammetry tools to build a 3D model of any item ([92]). In theory, the captured 3D models could be compared with existing CAD files or models of protected items in order to find possible matches. A number of services can already compare 3D models to find similarities or differences ([93]). Although integrated solutions do not currently exist, they could be developed on the basis of existing technologies in the future.

([89]) Paul Hanaphy 'Are 3D printed watermarks a "grave and growing" threat to people's privacy?', article in *3D Printing Industry*, September 2020.
([90]) European Commission's study on 'The Intellectual Property implications of the development of industrial 3D printing', carried out by Bournemouth University', February 2020. See also Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020, p. 13.
([91]) See Maker's Muse, 'How to defeat an STL Watermark (but would anyone really do this?) Watermark3D Round 2', December 2017.
([92]) See, for example, Trnio app.
([93]) See, for example, Transmagic CAD comparison or Capvidia CompareVidia.

4 Solutions to protect and manage copyright and neighbouring rights on content-sharing services

4.1 Challenges

The use of content-sharing services ([94]) has increased sharply in the last decade, with '[v]ideo-sharing platform services providing audiovisual content which is increasingly accessed by the general public … and social media services, which have become an important medium to share information and to entertain and educate, including by providing access to programmes and user-generated videos' ([95]). Alongside services allowing the sharing of all types of content, more specialised services focusing on specific types of content have also developed (e.g. for sharing scientific publications).

The large amount of copyright-protected content shared on these services has raised many questions over how to protect, manage and value copyright and related rights with high accuracy and short delays. It has also raised questions on ways to find the right balance between the respective interests and rights of IP owners, amateur creators, users and content-sharing services.

Some of these questions have been addressed by Article 17 of Directive EU/2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market. This article provides for a specific liability regime according to which online content-sharing service providers within the meaning of the Directive perform an act of communication to the public, and need to obtain an authorisation from the relevant rights holders for the content uploaded by their users on their services.

In cases where no authorisation is obtained and in order to avoid liability for copyright infringement, the service providers have to demonstrate that they have made their best efforts to obtain an

([94]) Directive (EU) 2019/790 on Copyright in the Digital Single Market, 17 April 2019. Article 2(6) defines 'online content-sharing service provider' as the provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes.

([95]) Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. Recital 4.

authorisation and to ensure the unavailability of specific works previously identified by rights holders ([96]).

In June 2021, the European Commission issued guidance on the application of Article 17 ([97]), pointing to ACR tools as one of the technical solutions that may be used to identify specific copyright-protected content for which rights holders have provided relevant and necessary information to online content-sharing service providers ([98]).

This use case provides several examples of the use of ACR technologies and related technological solutions in the context of content-sharing services. It mainly focuses on **fingerprinting-based solutions** to recognise content and protect and manage associated rights.

- It only partly covers the use of ACR solutions by IP owners to detect unauthorised uses of their content on online services (e.g. by scraping publicly accessible services to identify infringing content) and take action (e.g. by sending a notification of the IP infringement to the relevant service).

- It does not cover hashcode-based solutions, which are less resource-intensive and can, for example, be used in conjunction with fingerprinting-based solutions to detect strictly identical files that have been previously identified and have the same hashcode. Files previously identified this way do not need to be run through the fingerprinting system again ([99]).

- It does not cover the streaming of live events on content-sharing services (e.g. concerts or sports events), which gives rise to different types of challenges and is the focus of use case 5 (see Section 5).

([96]) Directive (EU) 2019/790 on Copyright in the Digital Single Market, 17 April 2019. Article 17(4).

([97]) See European Commission, Guidance on Article 17 of Directive (EU) 2019/790 on Copyright in the Digital Single Market (4 June 2021), p.20.

([98]) For a further interpretation of Article 17 of the C-DSM, see case C-401/19, in which the Court of Justice of the European Union (CJEU) dismissed the action brought by Poland against that provision and confirmed that the obligation of online content-sharing service providers to review, prior to its dissemination to the public, the content that users wish to upload to their platforms, is accompanied by the necessary safeguards to ensure that such an obligation is compatible with freedom of expression and information (26/04/2022, C-401/19, Poland v Parliament and Council, EU:C:2022:297).

([99]) See Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020, p. 4.

This use case also explores how the parameters and rules of fingerprinting-based solutions and the development of AI-based systems can further improve content recognition and support the management of copyright and the application of exceptions and limitations (see Section 4.2.2).

4.2 ACR technologies and technical solutions in use

The identification of content using fingerprinting-based solutions, and subsequent action(s) takes place in several steps.

- A **reference fingerprint of each piece of content to be identified** is created and added to a reference database. Metadata, including rights management information for each piece of content, is added alongside the reference fingerprint.

- A **fingerprint is created of any piece of content uploaded** on the content-sharing service and compared with those present in the reference database.

- When a partial or total match between fingerprints is detected, **rights management rules based on associated metadata are automatically applied**, leading to specific actions like the monetisation or blocking of the content uploaded.

Beyond the identification of content, and the application of specific action(s), some of the solutions also provide **mechanisms to deal with complex IP rights management issues**, such as conflicts between several IP owners or between IP owners and users, reporting on the use of protected works to support the distribution of related remuneration.

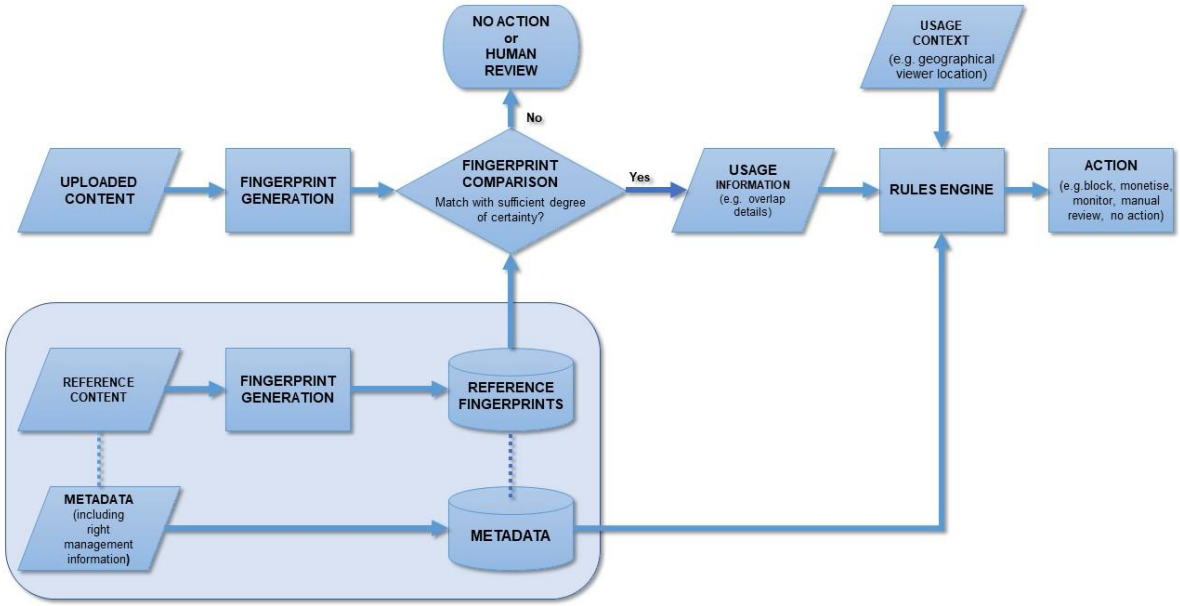


Figure 4: Example of a fingerprint-based ACR and content management workflow – Source: EUIPO, based on unpublished IFPI documentation.

Special focus on metadata

The upstream workflow of an ACR-based content management systems relies on **rights metadata or 'rights management information'**, which identifies any given work and its rights holder(s). In fingerprinting-based solutions, this metadata is associated with the reference content. As different solutions are developed, a number of challenges arise regarding the sources and quality of metadata – when it is not simply missing – and its interoperability. These seem to be caused by the several approaches to data identification and verification used to develop different sets of metadata ([100]). Although there are good practices developing with efforts in different sectors to standardise metadata, some challenges remain ([101]). These challenges, which affect the effectiveness of fingerprinting-based solutions, are not covered by this discussion paper. However,

([100]) European Commission, Directorate-General for Communications Networks, Content and Technology, Study on copyright and new technologies: copyright data management and artificial intelligence, 2022, p. 43.

([101]) Ibid. The European Commission study compiles information on the most important ongoing EU and industry initiatives to address some of the identified challenges related to rights metadata, such as data access and exchange – See Annex 3, 'List of current and ongoing initiatives in data interoperability within the context of rights infrastructure'.

they are covered in the study commissioned by the European Commission on '**Copyright and new technologies: *copyright data management and artificial intelligence***' ([102]). This study also explores existing initiatives to address these challenges and put forward possible avenues for future action in this area.

Fingerprinting technologies to protect and/or manage IP rights are developed by two main types of actors.

- **Content-sharing services** developing their own **in-house solutions** to support the management of IP rights by relevant rights holders regarding content uploaded by their users on their services. This typically includes the possibility to monetise these rights, monitor the use of content or block unauthorised content.

- **ACR solution vendors or service providers** developing and licensing the use of their fingerprinting-based solutions to content-sharing services. These solutions can be integrated directly into the system of the content-sharing platforms ('buy-in ACR solutions'), or provided to them as a service ('outsourced ACR solutions').

4.2.1 Types of content and ACR-based solutions

Fingerprinting is the ACR technology that seems to be most used for audio ([103]), video and audiovisual content.

([102]) Ibid. Among the different challenges related to rights metadata, the study notably looks at the availability of rights metadata attached to content, the interoperability between different systems for exchanging metadata, and the authority of metadata sources.

([103]) In the audio sector, traditional fingerprinting systems usually aim to recognise a particular sound recording. In addition, algorithms are available to recognise the 'composition' or 'melody' of a piece of music, such as Melody ID by Google. Such systems could complement the possibilities for right holders to control their rights. (See CSPLA/Hadopi/CNC, Mission report Towards more effectiveness of copyright law on online content sharing platforms : overview of content recognition tools and possible ways forward, 2020, p. 16, Content ID for music partners on YouTube Help, or Media rights management using melody identification on Google Patents).

In-house ACR solutions for audio and video content

Some content-sharing services have developed their own ACR technologies and content management systems that are used specifically for their services. This is the case of YouTube's Content ID ([104]), as well as Meta's Rights Manager ([105]), which use fingerprinting-based technology to allow IP owners to identify and manage their content on these services. IP owners who meet certain eligibility criteria ([106]) can provide the content management systems with their copyright-protected content to be converted into reference fingerprints and added to the databases, along with metadata covering rights management information (e.g. licensing terms or data on ownership of rights). New content uploaded by users on the content-sharing platforms, as well as already uploaded content, are scanned; if they are recognised, action is taken based on pre-defined rules set by the rights holder ([107]). Possible actions at the level of the content-sharing platform include blocking, monetising and monitoring the use of content. In some cases, human reviews are also possible.

In addition to content recognition and management, some of these systems include mechanisms for handling conflicts between IP owners regarding rights on a specific piece of content ([108]), and for handling disputes with users ([109]).

Buy-in or outsourced ACRs for audio and video content

([104]) See 'How Content ID works'.

([105]) See Rights Manager website and 'Facebook Rights Manager' | EC stakeholders dialogue on Article 17 of Directive EU/2019/790 (16 December 2019).

([106]) See, for example, 'Quality for Content ID' or 'Eligibility for Rights Manager'.

([107]) See **Error! Reference source not found.** for an overview of the process, and the section below on rules and complementary technologies for more information about rules.

([108]) For example, conflicts over asset ownership happen when multiple content owners assert over full ownership of an asset in a specific territory. YouTube, for example, provides an option to remove ownership of the asset in a particular country, request an ownership transfer, or contact the content owners. See YouTube, 'Resolve asset ownership conflicts'. Meta's Rights Manager has a similar process. See 'Conflicts in Rights Manager'.

([109]) Users uploading content are able to dispute copyright infringement claims through counter notification. For example, following YouTube's counter notification procedure, if the notifier does not respond within 30 days to the counterclaim, the claim expires and the notified content is reinstated. If the notifier can uphold the claim, the content remains unavailable for the duration of the dispute. See 'Dispute a Content ID claim - YouTube Help'. Importantly, under Article 17(9) of Directive EU/2019/790, Member States have to provide that online content-sharing platforms put in place an effective and expeditious complaint and redress mechanism to address disputes over the disabling of access to, or the removal of, works or other subject matter uploaded by their users.

A number of ACR solutions providers license their services to content-sharing services. For example, Audible Magic([110]) licences a fingerprinting-based copyright management solution to a number of content-sharing services. In this case, IP owners are not in direct contact with the content-sharing service but deal with the ACR service provider to identify the content they wish to protect. The ACR service provider generates and manages reference fingerprints and associated metadata, which are compared with the fingerprints for content uploaded by the users of content-sharing service platforms. In the case of a match, the service provider applies the rules pre-defined by the right holder(s), as set in the associated metadata.

In this context, ACR is a central component of rights protection and management solutions and supports other services offered to content-sharing platforms, such as content licensing, licence administration, matching licences to content, or royalty administration. The cost of the service is borne by the content-sharing service, and there is no direct financial relationship with the IP owners([111]).

Another example of a fingerprinting-based solution is Pex([112]), which offers a set of copyright protection and management services, one of these being its 'Attribution Engine' solution. The solution scans users' uploads prior to publication on content-sharing services that use it for copyright-protected audio and audiovisual content. In addition to allowing right holders to identify, monetise or control how their protected content appears on the platform, the solution provides video and audio analytics. Pex also provides a separate 'Discovery' solution that scans content already published online across dozens of platforms that do not use its Attribution Engine, and provides this data and analysis to the relevant rights holders.

In the absence of fingerprinting standards, and with the development of separate systems used by different content-sharing services, it is a challenge for rights holders to submit and update reference files for their content across the different systems. In this context, a partnership agreement was developed in 2017 in France between the French anti-piracy group Association de lutte contre la

([110]) See Audible Magic website.
([111]) See Audible Magic Corporation, 'Powering the Compliance and Licensing of Copyrighter content on social video networks', (slide 3), ref. Ares(2017)4595074 (2017).
([112]) See PEX website and PEX presentation at stakeholder dialogue on Article 17 of Directive (EU) 2019/790 (at 12:03:50).

piraterie audiovisuelle (ALPA) and Google – and then with Meta (Facebook) ([113]) – under the umbrella of the French Centre National du Cinéma et de l'image animée (CNC). The agreement provides a 'one-stop shop' solution for rights holders to use YouTube's Content ID, with the goal of extending it to other services ([114]). Some private initiatives are also developing to provide services to rights holders to register their content with multiple content recognition services.

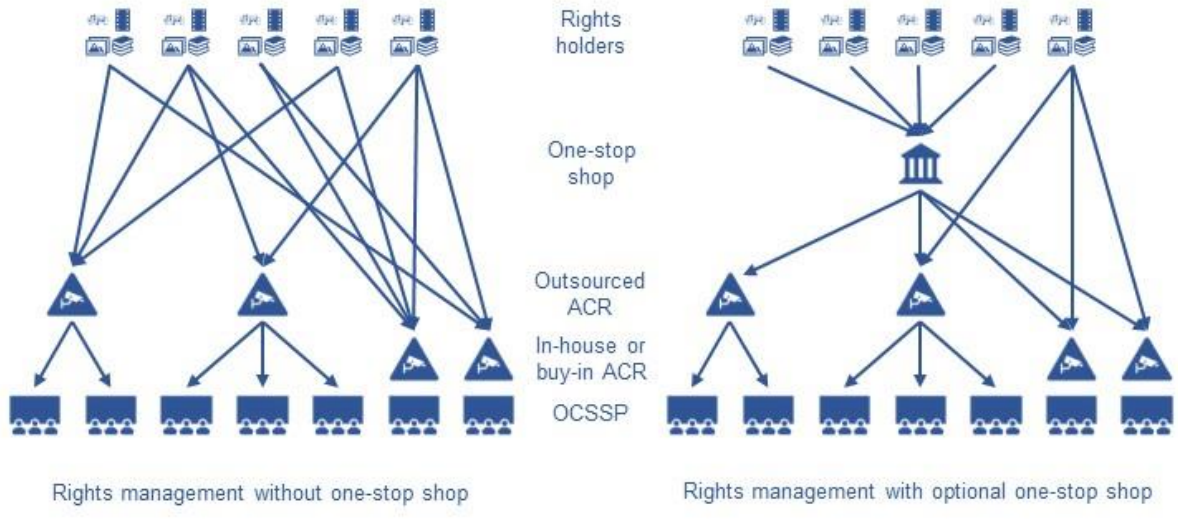


Figure 5: Processes to submit reference files with and without one-stop shop – Source EUIPO

ACR-based solutions for image and photographic content

A few companies provide ACR-based solutions for image and photographic content. For example, Videntifier ([115]) provides a visual search engine solution designed to deliver different services for law enforcement authorities ([116]), IP owners, and advertisers. It is a fingerprint-based image recognition tool ([117]) that also recognises images within videos. The cost of the solution is based on the volume

([113]) See 'Le CNC et l'ALPA salient l'engagement de Facebook dans la lutte contre le piratage', July 2021 (French only).
([114]) See 'Social Media – Discussion paper: New and existing trends in using social media for IP infringement activities and good practices to address them', EUIPO, June 2021, p. 29.
([115]) See Videntifier website.
([116]) In 2013, Videntifier Technologies signed an agreement with Interpol to provide advanced imaging technology in the effort against child sexual abuse material. In 2009, Microsoft developed PhotoDNA, a technology that aids in finding and removing known images of child exploitation.
([117]) See F. Ásmundsson, H. Lejsek, K. Daðason, B. Þ. Jónsson, L. Amsaleg, 'VidentifierTM Forensic:Robust and Efficient Detection of Illegal Multimedia', 2009.

of video or images to be validated, but also on the size of the reference database to be used as the validation set.

In addition, some content-sharing services providing public access to all types of content are developing their own in-house solutions. This is the case for Meta, which, in September 2020, announced the introduction of Rights Manager for images to help IP owners to protect and manage their images and photos across Facebook and Instagram, including when social media posts with images are embedded on third-party sites. This ACR system functions in the same way as Meta's Rights Manager for video ([118]).

Some companies also provide watermarking-based solutions. This is the case for IMATAG ([119]) and Digimarc ([120]), which provide IP owners with an invisible watermarking solution that can make copyright-protected images traceable before uploading them to content-sharing services. This solution is able to detect the original source of the upload with a reverse image search, to track where and how the content was shared, and report data on how the content was used by users of the content-sharing services. The pricing of these solutions depends on the number of images to be watermarked.

Combined watermarking and fingerprinting can be used by IP owners for external scans of content-sharing services in order to protect copyright, as well as for reporting and handling licence income distribution (e.g. by collective rights management organisations).

ACR-based solutions for the publishing sector

ACR-based solutions are not widely used on content-sharing platforms with regard to content from the publishing sector, including books, newspaper articles, scientific publications, or comics. Audiobooks may be an exception, as audio fingerprinting can be used on this type of content.

([118]) See Facebook Newsroom and Techcrunch.
([119]) See IMATAG website.
([120]) See Digimarc website.

ACR techniques to identify the content of text or documents, including forensic watermarking ([121]), do exist ([122]). Identifying identical text content is far less complex than identifying identical audiovisual content, and detecting plagiarism can be improved by using AI ([123]). However, identifying possible copies of plots in the realm of fictional works remains quite difficult ([124]) ([125]).

Scribd has developed BookID – a solution based on digital fingerprints generated from semantic data analysis of texts – which scans uploaded documents and removes those that have the same, or a substantially similar, fingerprint as one stored in a reference database ([126]).

Some publishers of scientific content have suggested that content-sharing services use systems like Crossref ([127]) to help identify rights to content. For example, content-sharing services could check Digital Object Identifiers associated with articles against databases provided by publishers that give information on usage rights to publications. Since this type of solution is only based on the use of metadata, it is out of the scope of this analysis.

4.2.2 ACR solutions supporting the management of copyright and application of exceptions and limitations

Depending on the type of content, multiple IP rights may apply to a single piece of protected content (e.g. audiovisual content), and some of its uses may be covered by copyright exceptions and

([121]) For example, a text can be watermarked by playing with imperceptible spacing or the level of darkness of font.

([122]) See Rakesh Kumar Mishra, 'Deterring Text Document Piracy with Text Watermarking', in 'Digital Rights Management: Concepts, Methodologies, Tools, and Applications', by Information Resources Management Association, published by IGI Global, 2012.

([123]) See 'Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP'', November 2020, p. 24.

([124]) See Article 17 of Directive (EU) 2019/790 stakeholder dialogue, in particular the presentation by Wattpad during the fourth meeting.

([125]) Some technologies, initially related to potential disinformation, specialised in the analysis of similarities (or discrepancies) between different texts, such as the Newsback tool made for information tracking and authentication. When applied to copyrighted content, such technology could help to recognised copies of protected content.

([126]) BookID is currently limited to computer-readable text. BookID cannot currently detect images, illustrations, and sheet music. See 'About the BookID Copyright Protection System'.

([127]) See Crossref website and Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes, Bundesministerium für Justiz und Verbraucherschutz (German), RELX p. 10 and Öffentliche Konsultation zur Umsetzung der EU-Richtlinien im Urheberrecht (DSM-RL (EU) 2019/790 und Online-SatCab-RL (EU) 2019/789) , ResearchGate p. 12.

limitations. This leads to situations where the application and management of copyright and neighbouring rights can be complex and cannot be fully automated.

As provided by Directive (EU) 2019/790; '[t]he steps taken by online content-sharing service providers in cooperation with rightholders should be without prejudice to the application of exceptions or limitations to copyright, including, in particular, those which guarantee the freedom of expression of users' ([128]). As a result, content management systems may have to take into account the context in which copyright-protected content is used, and that use may be covered by an exception or a limitation.

During the stakeholder dialogue on Article 17 of Directive (EU) 2019/790 ([129]) most participants agreed that, in the present state of the art, no content management system is able to automatically detect elements of context indicating that the use of a piece of copyright-protected content is covered by an exception, at least not with a sufficient degree of certainty. Therefore, human review remains essential in a number of situations where the respective rights and interests of rights holders and users need to be balanced.
However, given the amount of content to be manually checked on major content-sharing services, ACR systems may be parametered in a way that helps reduce or prioritise human reviews. In addition, the development of AI-based or enhanced ACR technologies has the potential to support human review by performing risk-assessment on the probability that the use of a copyright-protected content is covered by an exception or not.

([128]) See Directive (EU) 2019/790 on Copyright in the Digital Single Market, 17 April 2019, Recital 70 and Article 17(7), which provide that the cooperation between online content-sharing service providers and right holders to avoid unauthorised content, cannot lead to the unavailability of content which does not infringe copyright and related rights, due to the application of an exception or limitation. The aim is to ensure that 'legitimate uses' remain unaffected by such cooperation. See also European Commission, Guidance on Article 17 of Directive (EU) 2019/790 on Copyright in the Digital Single Market, 2021, p. 29 and Case C-401/19 (26/04/2022, C-401/19, Poland v Parliament and Council, EU:C:2022:297, § 85-86).

([129]) See Stakeholder dialogue on Article 17 of Directive (EU) 2019/790; See also European Commission, Summary Report on the targeted consultation on the application of Article 17, June 2021; See also European Commission, Guidance on Article 17 of Directive (EU) 2019/790 on Copyright in the Digital Single Market, 2021, p. 20.

Parameters and rules

As explained above, fingerprinting-based solutions used to detect audio and video content can be parametered in a way that affect the action they take when they identify part of a piece of copyright-protected content (e.g. blocking or monetising). These parameters can be used to manage multiple rights on a single piece of content or to allow a certain degree of tolerance in the use of copyright-protected content.

The following list gives examples of existing parameters and rules. They have been compiled from various fingerprinting-based solutions([130]), and not all options may be available in all systems. They can be used to determine the following.

- The degree of certainty that the reference fingerprint and that of the checked content match; the higher the level of certainty, the lower the risk of 'false positives'([131]).

- The extent of the overlap between the reference and the uploaded piece of content:
    - the length of time or percentage of an uploaded piece of content that is taken from the reference content;
    - the length of time or percentage of the reference content that is used.

  These parameters can be used to accommodate *de minimis* uses that exist in certain countries([132]).

([130]) Additional rules may exist, for example for classifying content. This list focuses on rules that can be relevant for triggering the action of blocking content uploaded by the users of a content-sharing service. Movilabs has published a suggestion for a specification providing a mechanism for rightholders to inform content-sharing services on how to handle their content, and which includes rules on content matching. See Movilabs, Content Recognition Rules, TR-CRR1, v1.1.1, 7 July 2008.

([131]) 'False positive' in this context is wrongfully identifying a piece of content as one included in the reference database and applying pre-defined action to it, (e.g. blocking or monetising). A 'false negative' is a piece of content that should be recognised but is not. Requiring a very high level of certainty can undermine the recognition of certain types of content (e.g. similar sounding piece of electronic music, or different audio books read by the same speaker).

([132]) For example, in the context of its transposition of the Directive on Copyright in the Digital Single Market, Germany has implemented quantitative threshold to determine whether the use of a work is 'presumably authorized by law'. Limited uses of protected works are covered by *a de minimis* use. Less than 15 seconds of video footage or sound, less than 160 letters of a text or images up to 125KB are assumed to be below the threshold. See Act on the Copyright Liability of Online Content Sharing Service Providers, p. 6, Section 10.

- The type of content that matches (e.g. audio, video or both). These parameters can be used to manage the different rights on a single piece of content, and ensure that a piece of content is not monetised until all the required rights have been claimed.

- Geographical area(s) / viewer location(s) in which a given set of rules should apply. These parameters can be used where different right holders hold the rights for different territories and apply different rules.

- The type of access to the uploaded content (private or public) for which the rules should apply. These parameters can be used to limit the use of a piece of content to a private setting.

- The type of account that publishes the uploaded content (e.g. private person, official page of an organisation, or whitelisted account). These parameters can be used to whitelist the accounts of users that may benefit from copyright exceptions for certain uses of a protected piece of content (e.g. public institutions).

- Which segments of a reference file to exclude, for example if a rights holder does not have the rights to all of the content in the file. These parameters can be used to manage the different rights on a single piece of content.

- Different rules evolving over time depending on the different windows of exploitation of a piece of content. These parameters can be used to manage the use of a protected piece of content over time to best value access to it.

AI-based or enhanced ACR technologies to improve the recognition of content and analyse the context in which it is used

The first phase of this analysis of ACR technologies has identified several AI-based or enhanced ACR technologies that can be used to identify content or elements of a piece of content ([133]). Other papers have also analysed more specifically how such technologies can be used to protect and

([133]) Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020.

manage copyright ([134]). In the future, these kinds of solutions may improve content recognition, but may also allow analysis of the context in which a specific piece of content is used.

- **Computer vision and image recognition/analysis**

  Computer vision focuses on the processing of signals that represent images, training computers to interpret and understand the visual world. It can be used for a broad range of purposes, including facial recognition or image classification, or to produce metadata of image and video content based on identified elements. Computer vision not only enables systems to derive meaningful information from visual inputs, but also to take action or make recommendations based on that information. When analysing video content, the image recognition phase can be preceded by the detection of the most relevant images to be analysed in a piece of content, reducing the resources required.

  Different sub-fields of image recognition are of particular interest in the context of this use case.

  - **Logo recognition** is a specific category of image recognition (see Section 1.2.1), which can also be used to support further analysis of audiovisual content based on, for example, logos and banners that are typically added by television channels, sport event organisers, or television programme producers to their content.

  - **Facial recognition** allows a computer to match a face with a pre-labelled one, as well as to understand and recognise emotions. Facial recognition can help identify a specific film by recognising the specific combination of actors performing in a specific scene. The use of this technology is widely debated due to its implications for privacy and personal data protection ([135]), and different legislations and requirements are being considered in several countries. This may affect the possibility of using the technology for content recognition, especially by content-sharing services operating across many jurisdictions.

([134]) See for example CSPLA/Hadopi/CNC, 'Mission report Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward', 2020, and EUIPO, 'Study on the impact of artificial intelligence (AI) on the infringement and enforcement of copyright and design', March 2022.
([135]) See, for example, 'Regulating facial recognition in the EU In depth Analysis European Parliamentary Research Service'.

- **Optical character recognition (OCR) and text recognition** make it possible to recognise and convert text from visual content into a raw text format. This enables further analysis of audiovisual content based on, for example, subtitles or text that is displayed in the media. AI-based or enhanced technologies can help overcome some typical obstacles in the fields of classic Optical Character Recognition (OCR) such as extracting text present in an image or extracting text from documents arranged in complex ways ([136]).

- **Speech recognition and natural language processing**: speech recognition makes it possible for a computer to convert speech into a digital text format. Advanced speech recognition supported by AI also allows a computer to distinguish a particular speaker's voice. Natural language processing refers to processing of the text to derive further information from it. It can be used for language identification and other purposes such as content extraction, classification or machine translation.

Some of these technologies are already in use by some content-sharing services to detect content that may be in breach of their terms and conditions and/or content policies (e.g. terrorist, pornographic, nude, or violent content), and can also be used to detect 'deepfakes' ([137]). For example, Meta ([138]) and Microsoft ([139]) have developed AI models that have been trained to be able to spot AI-manipulated audiovisual content ([140]).

In the future, these technologies may also support human reviewers' assessment of legitimate uses of a copyright protected piece of content uploaded on content-sharing services, and/or help in prioritising these reviews. For example, speech recognition and natural language processing could be used to analyse the comments added to a video in order to identify terms or patterns that are typically associated with the use of protected content covered by exceptions. Some academic research even suggests that with the further development of machine learning, copyright exceptions

([136]) See 'Learning to Read: Computer Vision Methods for Extracting Text from Images' , *Medium*, 2019.

([137]) Deepfakes are defined as 'manipulated or synthetic audio or visual media that seem authentic, and which feature people that appear to say or do something they have never said or done, produced using artificial intelligence techniques, including machine learning and deep learning'. See EPRS, 'Tackling deepfakes in European Policy', July 2021, p.2.

([138]) See Facebook AI, 'Reverse engineering generative models from a single deepfake image'.

([139]) See Microsoft blog, 'New steps to combat disinformation', September 2020.

([140]) See UNCCT-UNICRI Report on 'Countering Terrorism Online with Artificial Intelligence', p. 19.

could be potentially embedded in the system design[141] to identify uses covered by copyright exceptions or limitations[142]. However, although AI has great potential, it also has limitations and can be subject to bias depending on the parameters and datasets used to develop and train it. In this context, the reliability of the results it provides cannot always be guaranteed, making any future solution a support, but not a substitute, for human review.

4.3 ACR's potential and limitations

In light of the above developments, the following list suggests the potential and limitations of ACR when it comes to the protection and management of copyright and neighbouring rights on content-sharing services.

- **Improvement of IP protection and management through ACR**: by supporting the handling of large amounts of content with high accuracy and speed, ACR (in particular fingerprinting-based solutions) is a central technology for content-sharing services[143]. It enables:
    - recognition of content even when the content is modified and when other metadata or identifiers have been detached/stripped out;
    - persistent identification – the recognised content can be linked back to reference sources of metadata, including identifiers, tags, rights management information, etc.;
    - delivery, on a large scale and with high accuracy and robustness, of processes that would otherwise be fragile or manually intensive to implement[144].

[141] Professor Dan L. Burk further argues that a time gap will always exist between the latest judicial decision and the legal rules and outcomes that programmers manage to encode in the algorithms. Nevertheless, if automated fair use systems are constantly upgraded, the time lag between the two may be much more acceptable. See Dan L. Burk, 'Algorithmic Fair Use', 86 *University of Chicago Law Review* 283, 2019.

[142] For example, Professor Niva Elkin-Koren arguing that algorithms could learn to identify patterns of fair use instances by studying previously decided fair use cases. See Niva Elkin-Koren, 'Fair Use by Design', *UCLA Law Review* 22, 2017, https://ssrn.com/abstract=3217839; see also Professor Peter K. Yu, who suggests that automated fair use systems could be developed by first focusing on 'minimum essential levels of noninfringing uses'. 'Can Algorithms Promote Fair Use?', 14 *FIU Law Review*, p. 329-331, 2020.

[143] For example, in May 2019, more than 30 000 hours of content were uploaded to YouTube per hour. See 'Hours of video uploeaded to Youtube every minute as of May 2019' – Statista, 26 January 2021.

[144] Source: IFPI, unpublished document.

For example, a single midrange server can store up to 200 000 hours of reference video, and a single frame can be found within the dataset in 25-30 miliseconds([145]). In addition, as explained above, fingerprinting-based solutions can include specific rules and parameters that can be used to deal with situations when multiple IP rights apply to a single piece of protected content, and partially accommodate some copyright exceptions and limitations. As explained, the development of AI may have the potential to support human reviewers in assessing whether the use of a piece of copyright-protected content is covered by an exception or limitation, and/or prioritising content to be reviewed.

- **Data resources**: although very large content-sharing services have been able to develop their own solutions in-house, the majority of content-sharing services rely on fingerprinting-based solutions provided by third-party vendors. It is also very difficult to find reference datasets for training ACR systems, as the test beds are not shared by all companies([146]).

  According to Article 17(4) of Directive (EU) 2019/790, in the absence of an authorisation, IP owners will have to provide content-sharing service providers with all the 'relevant and necessary information' for them to take action and ensure the unavailability of specific copyright protected content from their service. Following the Commission's guidance, this information must be, as a minimum, accurate about the rights ownership of the specific works and must be 'necessary' so as to allow the service providers to apply effectively their technological solution, where used([147])([148]). It is expected that these data flows will feed into and enhance the datasets of content-sharing service providers, including those using ACR solutions. It should also improve the accuracy of the matching process. However, the

([145]) See 'Videntifier: Fast & Scalable Video and Image Identification' | EC stakeholders dialogue on Article 17 of Directive EU/2019/790 (25 November 2019)

([146]) See European Parliament Study, G. Sartor, A. Loreggia, 'The impact of algorithms for online content filtering or moderation', 2020, p. 52.

([147]) On the notion of 'relevant and necessary information', see European Commission, Guidance on Article 17 of Directive (EU) 2019/790 on Copyright in the Digital Single Market (4 June 2021), p. 12. What may constitute 'relevant and necessary information' will vary depending on the work in question, the circumstances and the solution deployed by the content-sharing services. If fingerprinting is used, the right holders may be asked to provide a fingerprint of the work, or a file, together with information on the ownership of the right.

([148]) Some EU academics suggested using the exchange of information between IP owners and online content-sharing platforms under Article 17(4) C-DSM to progressively create an EU copyright data repository offering comprehensive, accurate and interoperable information on works and rightsholders. See Martin Senfteben and cie, Ensuring the Visibility and Accessibility of European Creative Content on the World Market - The Need for Copyright Data Improvement in the Light of New Technologies and the Opportunity Arising from Article 17 of the CDSM Directive, February 2021.

efficiency of this mechanism will depend on the implementation of this provision and the cooperation between the relevant actors.

- **Accuracy**: fingerprinting-based solutions typically support the detection of content even if it has been distorted, flipped or mirrored. This is also the case where coloured content is turned into black and white, or if some colours are shifted, as well as where the aspect ratio of an image is changed ([149]). As for audiovisual content, it is also the case if the content is slowed down or sped up or if the sound volume has been raised or lowered. However, the accuracy and level of certainty of such solutions also depends on the length of the uploaded content, with different systems having different minimum length to identify referenced content.

  In addition, while companies providing fingerprinting-based solutions typically claim very high accuracy rates ([150]), one of the key challenges remains avoiding 'false positives' ([151]), where a piece of content uploaded on a content-sharing service is wrongly matched with content stored in the reference database and improperly blocked or monetised ([152]). False positives can be a particularly acute challenge for certain types of content, for example different interpretations of a piece of classical music that is in the public domain. False positives also raise issues if/when they undermine the fundamental rights of users, such as freedom of speech.

- **Other factors**: the lack of standards and interoperability between different fingerprinting-based solutions is a challenge, as it leads to situations where IP owners have to submit their content or related fingerprints to different content-sharing services and/or solutions providers,

([149]) See 'Youtube Copyright Management Product Suite', EC stakeholders dialogue on Article 17 of Directive EU/2019/790, 2019, slide 12.

([150]) This is notably the case of Audible Magic with declared accuracy rate of 99.9 %; see Audible Magic Corporation, 'Powering the Compliance and Licensing of Copyrighter content on social video networks', (slide 22), ref. Ares(2017)4595074, 2017; see also 'Audible Magic Content Identification for Compliance and Monetization in Europe', 2017.

([151]) During the Article 17 of Directive EU/2019/790 stakeholder dialogues, it was mentioned that CMS / ACR systems are being optimised for handling blocking decisions and in particular to avoid false positives by all means. This standard may adversely impact other functionalities such as handling licensing issues. See GESAC/ SACEM presentation at EC stakeholder dialogue on Article 17 of Directive EU/2019/790 (at 16:50:29).

([152]) See T. Lester, D. Pachamanova, 'The Dilemma of False Positives: Making Content ID Algorithms more Conducive to Fostering Innovative Fair Use in Music Creation', 2017.

with no standardised interfaces or managing rules ([153]). In this context, the setting-up of one-stop shop systems could contribute to making the process easier to handle for IP owners (see Section 4.2.1). Non-interoperable databases of rights management information can also become an obstacle to data sharing and lead to ownership disputes, inaccurate attribution to right holders or duplicate claims. This is part of the global challenge put forward in the European Commission Study on copyright and new technologies, relating to the upstream lack of common and transparent rights metadata (or rights management information) framework ([154]).

Another challenge is the application of particular copyright exceptions or limitations to content uploaded by users that can be difficult to assess by technology. In most instances it requires a human review process that should allow both IP owners and users to express their views. Wrongful or abusive claims of rights on content also pose a particular challenge, as they can result in the removal of perfectly legitimate content.

Those challenges are addressed by some companies deploying fingerprint-based solutions through the possibility for users uploading content to dispute the claim ([155]). In this respect, the setting-up of effective and expeditious complaint and redress mechanisms by content-sharing services will offer additional safeguards for both users and the content-sharing services ([156]). According to Article 17(9) of Directive EU/2019/790, and the Commission's guidance, under these mechanisms, the decisions to disable access to or remove uploaded content will be subject to human review to determine whether the use is legitimate or not and should be restored or not ([157]). In addition, if users want to contest the content-sharing service

([153]) Setting up one-stop shop solutions like the service offered by the French association ALPA can contribute to make the process easier to handle for right holders, in particular for smaller ones.

([154]) See footnote 100. The study provides different avenues for future action including awareness initiatives and a cross-sector rights data network, and reports on other suggestions from the study teams towards an Open Rights Data Framework (Annexes 6-7). See European Commission, Directorate-General for Communications Networks, Content and Technology, Study on copyright and new technologies: copyright data management and artificial intelligence, 2022, p. 334 and s.

([155]) For example, according to YouTube's Copyright Transparency Report, 'Uploaders have filed counter notifications in response to over 5 % of removal requests from the first half of 2021 made through the webform, whereas it's fewer than 2 % for both Enterprise Webform and for Copyright Match Tool. Fewer than 1 % of all Content ID claims made in the first half of 2021 have been disputed, though when they are, over 60 % of disputes were resolved in favor of the uploader'. See YouTube Copyright Transparency Report H1 2021, p. 6.

([156]) See Article 17(9) Directive EU/2019/790.

([157]) Ibid. See also European Commission, Guidance on Article 17 of Directive EU/2019/790 on Copyright in the Digital Single Market (4 June 2021), p. 25, and Case C-401/19, where the CJEU confirmed the compatibility of Article 17(4) of the

provider's final decision, they should be in a position to use alternative dispute resolution schemes, which Member States have to make available for such disputes to be settled impartially ([158]). This requirement could trigger the setting-up of a neutral copyright dispute resolution service with the support of technology solution providers ([159]).

C-DSM Directive with the EU Charter of Fundamental Rights. It ruled that the exclusion of measures that filter and block lawful content when uploading, is a clear and precise limit on the preventive measures that may be required under that provision, 'to prevent the risk which, in particular, the use of automatic content recognition and filtering tools entails for the right to freedom of expression and information of users of online content-sharing services'. (26/04/2022, C-401/19, Poland v Parliament and Council, EU:C:2022:297, § 85).

([158]) Article 17(9) of Directive EU/2019/790.

([159]) At international level, see for instance 'Pex partners with World Intellectual Property Organization Arbitration and Mediation Center providing first neutral copyright dispute resolution procedure', September 2021. This initiative aims to propose dispute resolution services regarding the use of copyright material on user-generated content platforms.

5 Solution to identify live streams of IP-protected content

5.1 Challenges

The development of live streaming services is bringing about major market opportunities, but also new challenges in preventing the illegal live streaming of sport events, concerts or other IP-protected content ([160]). Such illegal live streams typically take place through the following channels.

- **Illegal IPTV services**, which can be free or subscription-based, and available through applications, including mobile applications ([161]). It is estimated that in 2018, 3,6 % of the EU population streamed unauthorised IPTV, and that in 2019 there were 7.6 million subscriptions to illegal streaming platforms in the EU ([162]).

- **Open web streams**, which can be accessed through websites where users can watch the live event. From the users' point of view, these sites are the live event counterparts of classic piracy streaming sites where, for example, movies and TV series can be found.

- **Legitimate services providing their users with live stream functionalities**, such as video sharing platforms or social media. According to one analysis, over 41 million viewers watched illegally retransmitted streams during the 2018 FIFA World Cup on social media alone ([163]).

([160]) This use case does not cover the live streaming of promotional video/events for the selling of counterfeit goods, which is a new way for IP infringers to reach out to consumers.
([161]) In addition to websites, mobile applications are used for the illegal streaming of sport events, See EUROPOL, 'Illegal mobile application with more than 100 million users taken down in Spain' (11 March 2021).
([162]) European Parliament Research Service, Study on 'Challenges facing sports event organisers in the digital environment', December 2020, p. 11; EUIPO Study on 'Illegal IPTV in the European Union' – Research on online business models infringing intellectual property rights, phase 3, November 2019; see also press release from the European Parliament, 'Tackling digital piracy of live sport events and protecting organisers', April 2021.
([163]) See Kevin Le Jannic, 'Social Media Piracy – How to Fight Back', Viaccess-Orca, Oct 2018.

The illegal live streaming of sport events is considered by some as the greatest challenge threatening sports rights owners ([164]), with more than 362 million visits to sports piracy websites in January 2019 alone ([165]). A French study estimated the loss of earnings for the sports sector in 2019 due to illegal online consumption at least EUR 100 million for France alone ([166]).

In May 2021, the **European Parliament** adopted a resolution ([167]) on the challenges of sport events' organisers in the digital environment, calling on the European Commission to clarify existing legislation and to introduce specific provisions to improve the enforcement of IPRs for live sport events. The report suggests the possibility of issuing injunctions to request the blocking of access to or removal of unauthorised online live streams. It also highlights the need for further harmonisation of existing rules on notice and action procedures, and notably in the context of the Digital Service Act ('DSA'), as well as common criteria for the certification of trusted flaggers and the application of know-your-business-customer ('KYBC') obligations for relevant intermediaries 'to prevent their services to be abused to facilitate the illegal streaming of sport events'. The report also proposes the establishment of 'a common Union quality and technical reliability standard for software tools deployed by rights holders, intermediaries and other service providers, in order to identify illegal broadcasting of live sports events with a view to creating a certification scheme for "trusted flaggers"' ([168]).

5.2 ACR technologies and technical solutions in use

In this context, ACR technologies can contribute to detection and verification of, and enforcement against, illegal live streams. This analysis mainly focuses on **fingerprinting**, which supports the

([164]) See European Parliament's resolution of 19 May 2021 with recommendations to the Commission on challenges of sports events organisers in the digital environment (2020/2073(INL), May 2021, point 9.
([165]) See MUSO, Inside the complex world of illegal sports streaming.
([166]) See Hadopi, Etude de l'impact économique de la consommation illicite en ligne de contenus audiovisuels et de retransmissions d'événements sportifs, December 2020, p. 40 (French only).
([167]) See European Parliament's resolution of 19 May 2021 with recommendations to the Commission on challenges of sports events organisers in the digital environment (2020/2073(INL), May 2021.
([168]) European Parliament's legislative initiative procedure 2020/2073, May 2021.

recognition of an extract of a piece of content, and **watermarking**, which can be used to embed information within a video or audio signal([169]). These technologies serve different purposes.

- **Watermarking** can be used to identify the authorised stream of live content used as a source for the illegal stream (e.g. devices or user accounts) for further investigation (forensic watermarking). Watermarking can also take the form of embedding a visible overlay (e.g. a logo or text) on a video.

- **Fingerprinting** systems are deployed by services misused for live streaming illicit content to identify and suspend such streams.

The main developers of these solutions are the following.

- **Legitimate content-sharing and streaming services** develop their own in-house fingerprinting-based solutions to identify illegal live streams and interrupt them. In this context, they need to cooperate with IP owners to make sure that they can ingest reference live streams in their ACR systems, for identical illicit live streams from their users to be recognised. In addition, some content-sharing services collaborate with rights holders to define signals (e.g. use of certain keywords in the description of the live stream) that can be used to identify suspected IP-infringing live streams and have them removed.

- **Third-party vendors** develop and offer their solutions to IP owners and/or streaming services.

    - **Watermarking-based solutions** are mainly used for IP owners to identify the source of a leak at user or device level (user-ID) for investigation purposes, and can in some instances lead to the suspension of the identified device or user account (see Figure 3).

      Watermarking can also be integrated at broadcaster level (network-ID) or during post-production (owner-ID, identifying the producer or right holder) – in this case, a

([169]) See Dominic Milano, 'White paper: Video Watermarking and Fingerprinting', May 2012.

content-sharing platform could look for watermarks and block or monitor all videos coming from the broadcaster or from the rights holder in question.

Watermarks can also be used to identify a specific title or competition, each title or competition having its own watermark. However, in practice watermarking is not generally used by platforms to identify illegal live streams. This may be due to lack of standardisation of the different watermarking techniques, the possibilities of circumventing watermarking and their consequences, and the resources needed compared with fingerprinting solutions already in place.

- **Fingerprinting-based solutions** can be used by IP owners and/or streaming services to identify illegal live streams and take action (see Figure 4).

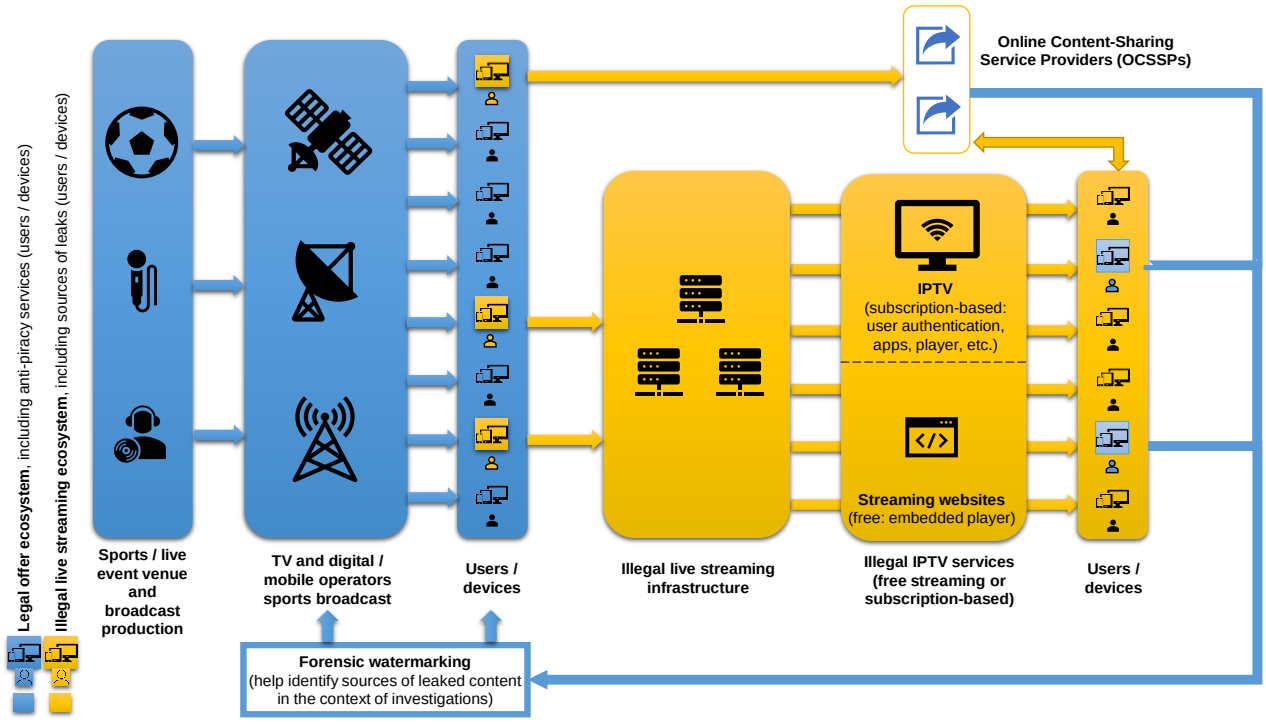


Figure 6: Forensic watermarking, live streaming ecosystems and data flows – Source: EUIPO

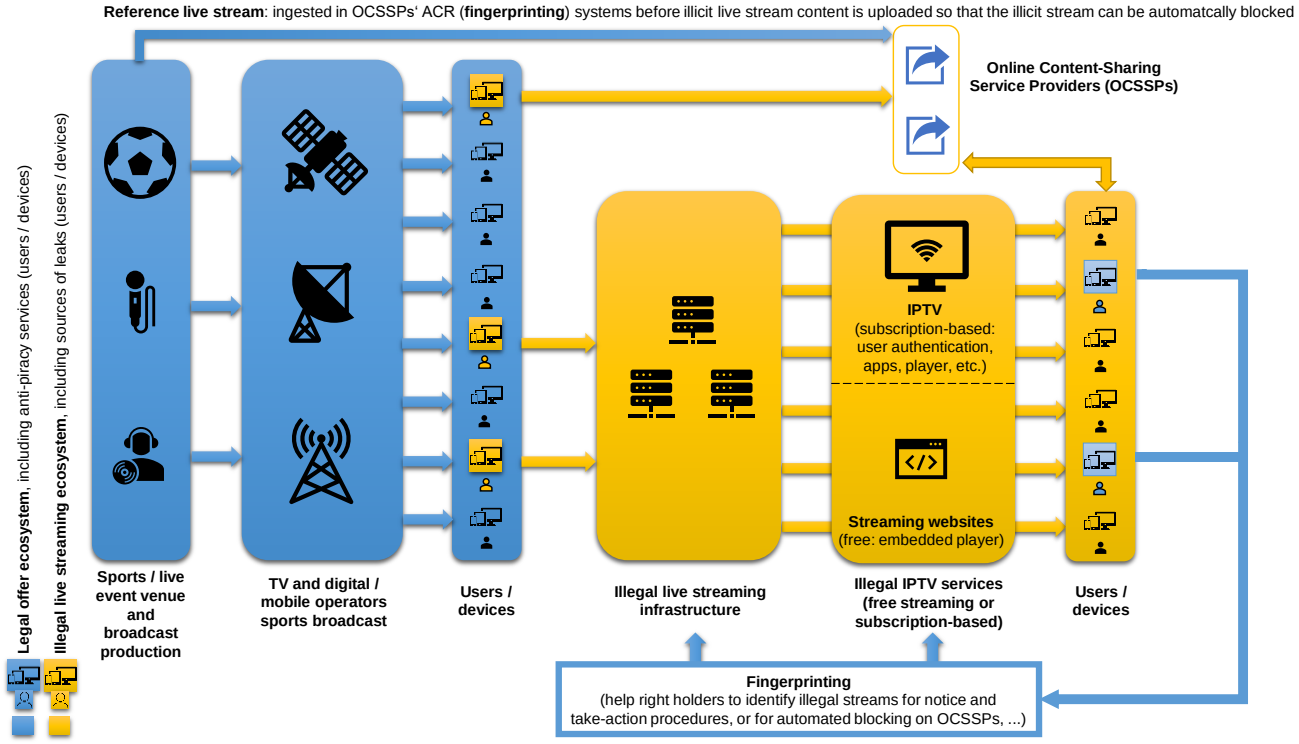


Figure 7: Fingerprinting, live streaming ecosystems and data flows – Source: EUIPO

Note on the ingestion of live streams: during the live event, the fingerprint is created 'on the fly', in consecutive pieces and sent to the reference database of an OCSSP as quickly as possible, for these partial fingerprints to be in the database before pirate restreams start to appear.

5.2.1 (Forensic) Watermarking

Digital content watermarking is the process of embedding additional information in the content, for example information about the copyright ownership and authorship. There are two main types of digital watermarking.

- **Visible watermarking** is where the embedded information is visible, usually as a text or a logo that identifies the IP owner of the content([170]). Visible watermarking is typically used to add information to identify the IP owner and prove IP ownership (e.g. broadcasters or Over-The-

([170]) For more information on reversible watermarking in copyright protection, see Jose et al., 'Copyright Protection using Digital Watermarking', NCACSA, 2012, p. 24.

Top ([171]) streaming services that stream protected content in real time), and can be used in the context of monitoring broadcasts.

- **Invisible watermarking** is where the embedded information is not perceptible. This solution can embed a hidden 'watermark' in the respective content in order to support the detection and monitoring of unauthorised uses ([172]). In live streams, forensic watermarking can be used to trace the device, network or user account that is leaking the content ([173]). Invisible watermarking can also be used to identify the original broadcaster of the content, even if the broadcaster's visible watermark/logo has been covered.

Forensic watermarking of streaming content makes use of specific techniques ([174]). Three main methods of video watermarking are currently in use: bitstream watermarking, A/B variant watermarking, and client-side watermarking, which all have different advantages and limitations when it comes to live content ([175]). An example of this type of watermarking is modifying the colour intensity of selected pixels without modifying the content. The invisible watermark is not perceptible and can only be revealed by specific watermark detection software.

In the context of this use case, **forensic watermarking provides a means to identify the source of leaked content** at the distributor, device or subscriber levels, as previously described. Watermarks that are invisible to the viewers are embedded in each distribution feed for identification (e.g. broadcasters or intermediaries as content-sharing platforms with live streaming functionalities). Embedding a watermark is just a first step that needs to be complemented by systems continuously monitoring content made available online worldwide and supported by 24/7 operations teams for monitored watermarked content to be detected no matter where, when or to whom it is distributed. Leaked content detected this way on piracy sites or IPTV services can be analysed for any embedded marks which, when extracted, provide information allowing distributor/device/subscriber

([171]) Over-The-Top (OTT) is a technical way of providing audiovisual content over the internet at the request of an individual user.
([172]) Jose et al., 'Copyright Protection using Digital Watermarking', NCACSA, 2012, p. 25
([173]) See Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020, p. 10; see also Dominic Milano, 'White paper: Video Watermarking and Fingerprinting', May 2012, p. 2; see also an article on TVTECH by Ali Hodjat, 'Securing the streaming of live sports and combating piracy', 2020.
([174]) See Streaming Video Alliance (SVA), 'Forensic Watermarking Implementation Considerations for Streaming Media', 2018, pp. 10 and 14.
([175]) See Akamai, 'Inside the World of Video Pirates', white paper, 2020, p. 18, or Friend MTS, 'Attacks on Subscriber Watermarking Technologies', white paper, p. 4.

identification depending on the marks present. This information can be used by investigative teams to locate the source of the leak and take immediate action or devise the best strategy to block future piracy activities.

Companies like NAGRA([176]), Viaccess-Orca([177]), Synamedia([178]), Friend MTS([179]) or Irdeto([180]) provide content protection solutions to IP owners that also use **invisible and inaudible watermarking**. These technologies can be used for live, non-live, OTT and broadcast distribution networks (for pre-recorded events or for live streaming). Some companies, for example Cartesian([181]), also specialise in services that test the robustness of watermark solutions([182]).

5.2.2 Fingerprinting

Audio/video fingerprints are based on unique characteristics of protected video and/or audio content, which are stored as 'fingerprints' in a dedicated reference database for comparison with fingerprints of unknown uploaded or streamed content to recognise and detect the use of copyright-protected content. An audio/video fingerprint can be a statistical content sample of the whole audiovisual content, or only part of it. Any video clip can be compared with the fingerprints stored in the database and checked to see whether there is a match between the fingerprints([183]).

Fingerprinting allows fast content identification. An important factor in successful fingerprinting technology is resilience to playout processing, such as aspect ratio changes, cropping, downscaling,

([176]) See NAGRA website.
([177]) See Viaccess-Orca website.
([178]) See Synamedia website.
([179]) See Friend MTS website.
([180]) See Irdeto website.
([181]) See Cartesian website.
([182]) It seems that some companies providing video-streaming services are also developing their own solutions. For example, in November 2020, Amazon filed a patent on a technology capable of tracking every single play of protected VOD included in Amazon's repertoire. The patented system assigns a unique identifier to each user and combines it with another code generated for each play on the content. This unique identification code (including the user's identifier and the identifier of the specific play) is embedded in an invisible watermark on the content. See USPTO PATENT 10 834 158, 10 November 2021.
([183]) See Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020, p. 16-17; see also Dominic Milano, 'White paper: Video Watermarking and Fingerprinting', May 2012, p. 5.

and bit rate reduction. Fingerprinting integrity must also withstand countermeasures used by video pirates to disrupt content protection; in addition, fingerprinting must work for all major video formats, as well as traditional and OTT delivery.

- **Fingerprinting solutions to take down content on content-sharing services**

  Some **ACR solutions are developed in-house by legitimate content-sharing services providing live streaming functionalities**, to detect illegal streaming of live events. YouTube's Content ID, for example, is also used to check live events streamed via YouTube for matches with copyrighted content. In this case, live feeds are ingested in real-time into the Content ID system. This includes live broadcasts such as sporting events or music festivals([184]). Some sports leagues, such as LaLiga in Spain, now use Content ID to automatically detect and block streams of their live matches on the online-content sharing service([185]). When content is identified in Content ID's database, a placeholder image may replace the live stream until the content is no longer detected. In some cases, infringing live streams may be terminated, and the YouTube channel owner may temporarily lose access to live streaming([186]). Meta's Rights Manager offers similar functionalities, and the company also partners with rights holders to support their live content enforcement strategies on its services([187]).

  Some **ACR solutions are developed by third-party service providers**. For example, Audible Magic launched AMLive™([188]), based on fingerprinting, to protect against rebroadcasting of premium content by users of live streaming platforms. Content owners, such as sport events' organisers, register their live event with Audible Magic and provide start and end times as well as a URL to get access to the legitimate broadcast feed. At the time of the event, AMLive takes the broadcast feed, creates digital reference fingerprints of the audio and video in real-time and stores them in the AMLive Registry. The streaming service sends the fingerprints of uploaded media or live broadcasts to the information service of Audible Magic, where they are compared to reference fingerprints in targeted reference databases. The

([184]) In 2018, for example, Fuji Rock Music Festival was streamed live on YouTube, and right holders used Live Content ID to keep unauthorised streams off the platform.
([185]) See 'LaLiga incorporates YouTube's Content ID tool into anti-piracy campaign', 2017.
([186]) See YouTube, 'Copyright issues with live streams'.
([187]) See UEFA committed to tackling audiovisual piracy during UEFA EURO 2020.
([188]) See Audible Magic, 'Audible Magic Launches AMLive™ to Protect Against Rebroadcasting Premium Content by Users of Live Streaming Platforms', 2018.

Audible Magic service returns results indicating a match or condition. In the case of a match, the content owner's pre-defined rules to block or allow the sharing of the content are communicated to the platform so they can be applied ([189]).

- **Fingerprints to take down content on illicit services**: several companies such as Vobile ([190]) or Webkontrol ([191]) offer video fingerprinting-based solutions to detect **illegal live streaming of events on illegal IPTV services or piracy websites**. The effectiveness of these solutions depends not only on the quality of the fingerprinting-based identification, but also on the capacity of its provider to find and detect potentially illegal streams to be analysed, and allow take down requests to be sent quickly when illegal re-streaming is detected.

  In practice, allegedly infringing live streams are verified using video fingerprinting technology, which matches detected re-transmissions to the pirate streaming server in real time. When illegal live streams are identified, the IP address of the pirate streaming server(s) is recorded. Analysis of the broadcasting infrastructure can give a clearer picture of the extent of the infringement and how best to counter it, and if needed be supplemented by human investigation. Finally, notifications can be issued to relevant intermediaries, in some instances automatically, to speed up the take down of the unauthorised retransmissions.

([189]) See Audible Magic, AMLive™ for Live Streaming Platforms, 2017.
([190]) See Vobile website.
([191]) See Webkontrol website.

Special focus on cooperation for live stream take-down processes

Identifying an illegal stream and its source using ACR systems is only a first step, as limiting the economic damage caused to the IP owners requires having it suspended as quickly as possible. This involves identifying and notifying the intermediary services used in the streaming, such as hosting and cloud providers (including hosting providers of streaming servers), internet access providers, or content-sharing services. Due to the time-sensitivity of live-streamed content, IP owners are typically seeking near-instant take down from the intermediary following a notice, and close cooperation with relevant intermediaries to develop streamlined notice and action processes.

This requires the IP owner and relevant intermediaries to agree on the information to be provided for a notification to be valid, on dedicated contact points and/or interfaces, such as dedicated portals to file such notifications, or application programming interfaces (APIs) that can be used for automating communication between the respective IT systems and programmes. Agreement may also need to be found on data formats and transmission protocols to be used.

A number of other issues are factored into the development of such cooperation, such as IT security, costs or checks and safeguards to avoid accidental overblocking and the potential infringement of users' rights and/or economic losses that may result from such overblocking. Additional costs and related compensation may also be factored in, for example, if human resources have to be available outside office hours to handle take-down requests.

5.2.3 AI-based or -enhanced recognition

AI-based solutions, and in particular object recognition, are also used by some content-sharing services providing live streaming functionalities, as another way to detect illicit live streams of IP protected events. The approach focuses on recognising a type of event that is typically protected by IP (e.g. a football match), as opposed to a specific event (e.g. football team A versus team B on a

particular date). It is combined with the analysis of a set of signals to trigger and prioritise human review that determines whether the stream is licit.

In practice, object recognition is run on a series of thumbnails from a live stream to detect relevant objects, and estimate the probability for the stream to be related to a certain type of event (e.g. a football match). In order to address potential cases of legitimate uses, object recognition can be used in conjunction with users' behaviour and pattern analysis (e.g. verified users, newly created accounts, or increases in the number of viewers) with various probabilities assigned to each behaviour. Once a certain threshold is reached, parameters help to narrow down the number of potentially infringing streams and submit them for human review. Logo recognition might also be used in the process of detecting sources of live streams to identify the rights holder before taking any action against the source.

5.3 ACR's potentials and limitations

- **Improvement of IP protection through content recognition**: modern content recognition technology is important for protecting the revenue of a premium live sports broadcast or streaming service, as protecting live sports events with digital rights management (DRM) and other technologies alone may not be enough to block piracy services and live sports event retransmission. Indeed, pirates frequently manage to effectively bypass protection measures to re-stream live sports content using various circumvention methods and tactics.

  Forensic video watermarking technology is an element of content security systems and anti-piracy strategies. It enables the identification of the sources (distributors/devices/users) of illicit streams. The information collected can subsequently be used in investigations, as well as to devise the best strategy to prevent future piracy activities. However, there are a number of techniques and strategies to circumvent watermark-based ACR solutions in general ([192]). When it comes to the circumvention of forensic watermarks applied to live content, IP infringers might also try to circumvent them by using hacked accounts or devices on which the watermarking tools are not implemented. They can also randomly switch between multiple accounts through

([192]) Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP', November 2020, p. 13-14.

the illicit live stream to undermine detection and/or use backup accounts to quickly replace disabled accounts.

Fingerprinting, and to a lesser extent watermarking, make it possible to identify illicit streams in real-time and on a large scale at the user facing end of the pirate broadcasting chain (e.g. on content-sharing services or illicit streaming sites). This is the base for further actions such as notice and action procedures or requests for blocking servers that stream pirated content.

In addition, different ACR techniques may be more or less resource- and time-consuming. For example, fingerprinting may be faster than forensic watermarking solutions for identifying content, and not all forensic watermarking solutions may be equally suitable for performing forensics on live streams.

- **Data Resources**: one challenge in the context of protecting live-streamed events, especially with fingerprinting solutions is to ingest the content into the ACR reference databases before illicit streams are broadcast. Achieving this may require specific agreements and technical setups between IP owners and ACR systems, in particular in-house ones([193]).

- **Combined use with other technologies**: protecting the legitimate streaming services with digital rights management (DRM) technology can contribute to reducing piracy by only authorising specific users to watch a specific live stream on a specific device, but there are situations where DRM is not the most effective solution, especially once the content has been pirated.

  For content-sharing platforms providing live streaming functionalities, the use of ACR can also be combined with user behaviour and pattern analysis, which can support the process of determining whether a stream is illicit.

([193]) It also requires a trusted relationship between the ACR solution provider and the IP owner that is sharing premium content to be fingerprinted.

Finally, ACR technologies can offer an efficient solution to detect illegal live streams on legitimate platforms and identify the device that is restreaming the content, and therefore allowing a timely shutdown of the illegal redistribution or other takedown actions ([194]).

([194]) See Dominic Milano, 'White paper: Video Watermarking and Fingerprinting', May 2012, p. 2; see also an article on TVTECH by Ali Hodjat, 'Securing the streaming of live sports and combating piracy', 2020; see also 'Forensic Watermarking Implementation Considerations for Streaming Media' by Streaming Video Alliance, July 2018.

Conclusion

The use cases show that various ACR technologies are already part of the tools supporting the protection of IP rights. In many instances, content recognition is just a core component of broader solutions that may, for example:

- lead to automated removal or notification of potentially IP-infringing content, and/or prioritisation for human review;
- combine the insights gained through ACR with context or behavioural information to refine the detection of IP-infringing content and activities; or
- support investigative work to identify the source of IP-infringing content and devise the best strategy to deal with it.

They also show that ACR technologies have the potential to address some of the challenges in protecting IP, such as the need for LEAs to have mobile solutions to detect counterfeit goods, or the need to trace the origin of a 3D model from its digital to its printed version.

Finally, they show that ACR technologies are also one of the tools supporting the management of IP rights. Content recognition is just part of the steps to decide on rules that should be applied to the content identified, and form part of broader systems to manage IP rights.

As ACR technologies and their application in the field of IP keep developing, the Observatory will continue to closely monitor evolutions in this field of technology.

List of Figures

Figures

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

ISBN 978-92-9156-326-5 DOI 10.2814/952694 TB-07-22-884-EN-N