EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

SOCIAL MEDIA – DISCUSSION PAPER

New and existing trends in using social media for IP infringement activities and good practices to address them

June 2021

DISCLAIMER

The views expressed in this discussion paper do not represent the official position of the EUIPO. This paper is based on the work of the EUIPO Observatory's Expert Group on Cooperation with Intermediaries. The views expressed in this discussion paper cannot be attributed to the Expert Group as a whole or to any single contributing expert.

The Observatory welcomes any further input or comments on this discussion paper, to continue deepening its understanding of good practices in undermining the misuse of social media for IP-infringing activities. This discussion paper may be subject to reviews or updates based on any further input from experts or new developments in the field.

ISBN 978-92-9156-296-1 doi: 10.2814/272629 TB-02-21-746-EN-N

Table of Contents

1 Foreword

The Expert Group on Cooperation with Intermediaries was set up to further the understanding of different intermediary services, how they can be misused for intellectual property (IP) infringing activities, and how these misuses can be undermined through good practices. Having looked at domain names in its first discussion paper ([1]), this second paper examines social media. It will hopefully contribute to a better understanding of how social media are misused to infringe IP or support IP-infringing activities, the challenges raised by this misuse, as well as existing and developing good practices through which they can be addressed.

2 Executive summary

Social media are online services combining a number of functionalities with different purposes (social connection, interaction and business) that support different levels of communication (public, semi-public and private) through different content formats. With the growing popularity of social media, IP infringers have developed new strategies to misuse their unique combination of functionalities for their own purposes.

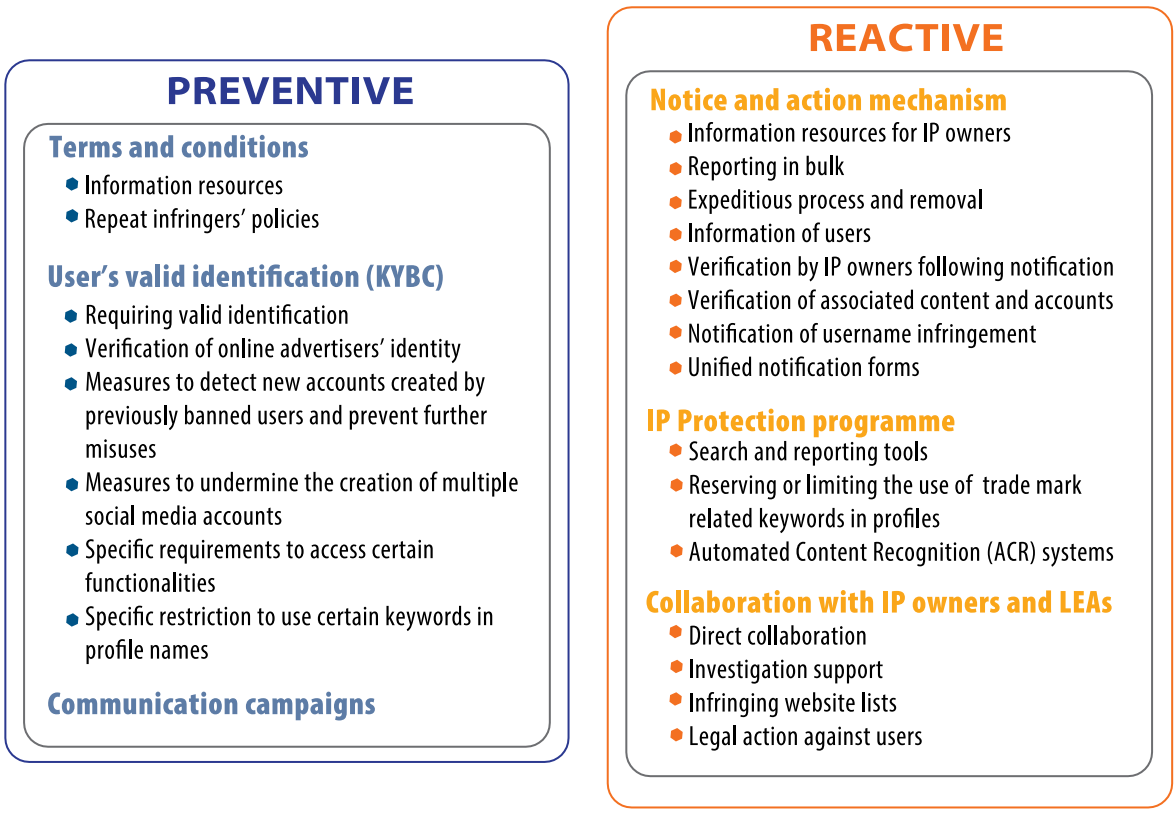
This discussion paper identifies a number of **new and existing trends**, with social media's functionalities being misused to infringe intellectual property rights (IPRs) directly, to support IP infringement through other channels, or to provide information on such activities. Some of the trends identified affect other online services as well, while others are specific to social media, with IP infringers:

- using social media's unique features to target and build an audience and to market their products and services through influencers, public posts and closed groups (i.e. invite-only groups);
- mixing social media's different levels of communication (i.e. public posts, closed groups and private communication) and using ephemeral content to defeat existing IP protection measures and investigation techniques.

([1]) EUIPO, Domain names – Discussion paper: Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP infringement activities, March 2021.

There are a number of **challenges** in addressing these trends, in particular the different regulatory frameworks applying to social media's functionalities supporting public or private communications. This limits the ability of IP owners, social media companies and law enforcement authorities to cooperate and take action, particularly when private communication functionalities are involved. IP infringers can take advantage of this by attracting users through innocent public content, inviting them to a closed group where they can promote their IP-infringing products or services, and then concluding the transaction through private messages.

A number of **good practices** are developing through which IP infringers' misuses of social media can be prevented or dealt with.



Some of these good practices address the misuse of generic social media functionalities enabling users to share content publicly (e.g. notice and action mechanisms or measures to prevent repeat infringements) and are relevant to most social media services. Others are more focused on specific business-related functionalities, such as ads or e-commerce functions (e.g. 'know your business customer' requirements and IP protection programmes) or to a given content format (e.g. automated

recognition of video content), and are only relevant to social media services offering these functionalities.

There are only a limited number of good practices that can address the misuse of social media's private communication functionalities or the use of closed groups. This is may be due to the legal framework that applies to these functionalities and limits the capacity of social media companies to cooperate with IP owners and law enforcement authorities. Therefore, special importance is attached to the good practices that have the potential to effectively undermine this trend, including notifications of IP-infringing content submitted by users and infringing website lists (IWLs).

If the good practices identified in this paper are implemented by 'traditional social media', the development of decentralised social media may well raise new issues and challenges that will need to be carefully monitored in the future.

3 Introduction and background

'Social media' is the term used to describe '[platforms] that [enable] end users to connect, share, discover and communicate with each other across multiple devices and, in particular, via chats, posts, videos and recommendations.' ([2]). Using social media websites or applications, users can create, co-create, discuss, and modify content that can be shared publicly or among their social connections.

Although a number of definitions of 'social media' have been put forward, none is a perfect fit, as the concept encompasses a broad range of services that may focus on different content formats ([3]) with different purposes, functionalities and target audiences. However, social media services tend to share a set of features.

- **User accounts or profiles**: They require their users to create an account or profile. This can be a prerequisite for access to the service or only to share content on it ([4]). Account creation requires users to accept and abide by the terms of use of the social media service.

- **User-created content**: They build on the creation and uploading of content by their users by hosting, indexing, enabling and encouraging the sharing of such content. While they do not control content shared by their users, they set rules on content that they do not deem acceptable on their services through their terms of use and additional rules or policies.

- **Social connections**: They allow their users to connect with and follow other users, and to develop and maintain a list of connections. This helps to determine how content is being shared by and displayed to social media users. Typically, content is shared with a user's connections or followers, and the user is shown content from those they are connected with or follow ([5]).

([2]) This definition is drawn from the Proposal for a Regulation on Digital Markets Act in relation to "online social networking platform" (Article 2(7) DSA proposal), issued by the Commission on 15 December 2020. It may therefore be subject to change during the legislative process.
([3]) Some social media services focus on text (e.g. Twitter), audiovisual content (e.g. TikTok) or audio content (e.g. Clubhouse).
([4]) A distinction is often made between 'profile-centric' and 'media-centric' services. 'Media-centric' services (e.g. YouTube) do not necessarily require a user to create an account in order to access content, but an account is required for posting or commenting on content.
([5]) Some social media services provide further options for sharing content with selected groups of users. See 'Public, private or selected group communication' below.

Some social media services also automatically suggest content to their users based on their interests or those of users with similar profiles.

- **Interaction with content**: They allow users to interact with content shared by others by re-sharing it, 'liking' it or commenting on it. A user's interactions can be relayed to their own connections or to a wider group through hashtags, supporting the spreading of content and information among a larger number of users.

- **Public, private or selected group communication**: They offer different ways for their users to share content or communicate. Users can choose to share content publicly, only with their social connections, or in some instances with selected groups of users. In many cases social media services also allow private communication among their users.

- **Ads/data-based business model**: Through users' content creation, social connections and interactions, social media services 'gain access to, collect and process information about users' socio-demographic profiles, interests and preferences. [They] use this data to create and offer paid advertising and other services that rely on highly granular and customizable user targeting options.' ([6]) ([7])

The six most popular social media services now have more than 1 billion users each worldwide ([8]). The number of social media users keeps growing in the EU with 65 % of internet users participating in social networks in 2019 and reaching nearly 90 % among 16- to 24-year-olds ([9]). With the growing popularity of social media services, IP infringers have developed new strategies to misuse the functionalities they offer to promote, sell or facilitate access to counterfeit goods and pirated content, or support other fraudulent activities such as phishing or gaining access to private information. All such misuses violate social media policies, and some services are developing specific tools and working with IP owners to address these issues. This also raises new challenges for and growing concern among IP owners and enforcement agencies alike.

([6]) European Commission, Behavioural study on advertising and marketing practices in online social media, June 2018.
([7]) Some services are developing other business models in parallel. This is notably the case with 'checkout' systems, which let professional or official brand accounts display their products and allow social media users to buy them directly through the service's own user interface and payment system.
([8]) https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.
([9]) European Commission, Digital Economy and Society Index Report 2020 – Use of Internet Services and Report 2019.

According to the *2017 Situation Report on Counterfeiting and Piracy in the European Union*, '[t]he use of social media for advertising counterfeit products is expected to continue in the future' ([10]). The *Intellectual Property Crime Threat Assessment 2019* also highlighted the fact that '[i]n recent years, social media marketplaces in particular have emerged as a key platform from where counterfeiters can access high numbers of consumers looking for counterfeit items with a generally low risk of law enforcement detection.' ([11])

As a result, some law enforcement agencies have started taking action against IP-infringing activities on social media. Notable examples are the 2015 Operation Jasper in the United Kingdom, which targeted social media sellers of counterfeit goods ([12]), or Operation Aphrodite, led by Europol ([13]). As Europol reported in the context of its operation, '[vendors] advertise the counterfeit goods through posts showing the product and price. Then, the details of the transaction are defined through other communication channels. Couriers deliver the packages and payment is made via prepaid cards or PayPal' ([14]).

Some IP owners are also considering that social media are becoming a primary channel for accessing film and television content and livestreamed events, including IP-infringing content ([15]). Operators of infringing services capitalise on the audience traffic to social media and misuse them to advertise their services and illegally redistribute content. The EUIPO's *Monitoring and analysing social media in relation to IP infringement* report, released in April 2021, was a first attempt to assess the extent to which social media are used to support recurrent IP infringement for both physical products and digital content. The report shows that, out of a total of 3.9 million public conversations related to categories of products and digital content, 11 % could possibly be related to counterfeit goods, and 35 % to piracy ([16]).

([10]) Europol and EUIPO, 2017 Situation Report on Counterfeiting and Piracy in the European Union, p. 53.
([11]) Europol and EUIPO, Intellectual Property Crime Threat Assessment 2019, p. 37.
([12]) Europol and EUIPO, op. cit., p. 16.
([13]) We refer here to Operation Aphrodite 2018, 2019 and 2020.
([14]) Europol, Social Media Crime: 20 000 packages of counterfeit medicine, mobile phones, jewellery, sunglasses and watches seized, May 2018.
([15]) For example the Nordic Content Protection identified Facebook pages related to illegal IPTVs with 1.3 million followers (See NCP, Annual Report 2020, p. 18).
([16]) EUIPO, Monitoring and analysing social media in relation to IPR infringement report, April 2021. This report investigates and quantifies the role that certain social media platforms unwittingly play in sharing, marketing, selling, promoting and/or advertising IP-infringing goods, works, materials and/or services.

According to a 2019 report by Hadopi in that year, 33 600 posts on Twitter and Facebook concerned access to illegal content, and Facebook groups and pages dedicated to illegal content were 'only followed by 5 800 followers or subscribers, on average'. Moreover, 15 % of copyright-infringing consumers claim to visit a social network frequently (at least once a month) to find illegal content ([17]).

Despite IP owners' growing concerns ([18]), initial desk research showed that there is still limited research into and analysis of IP-infringing activities on social media. As part of its Work Programme, the Observatory is updating its research into online business models that infringe intellectual property rights ([19]) and will look more specifically at business models involving social media. In parallel, for the purposes of this discussion paper, the Observatory has asked its Expert Group on Cooperation with Intermediaries to explore new and existing trends in the misuse of social media to infringe IPRs, the challenges these raise and the existing and developing good practices through which they can be addressed.

([17]) Hadopi, The illicit ecosystem of digital cultural goods, p.65; Hadopi, Accès illicite à des contenus culturels via les réseaux sociaux (October 2019, French only).
([18]) These concerns are reflected by the Commission in the Counterfeit and Piracy Watch List, December 2020.
([19]) EUIPO, Research on Online Business Models Infringing Intellectual Property Rights, Phase 1, July 2016; EUIPO, Research on Online Business Models Infringing Intellectual Property Rights, Phase 2, October 2017; EUIPO, Illegal IPTV in the European Union – Research on Online business models infringing Intellectual Property Rights, Phase 3, November 2019.

4 Trends

Experts identified a number of trends in the misuse of social media functionalities to infringe IPRs directly (see Section 4.1), to support IP infringement through other channels (see Section 4.2), or to provide information on such activities (see Section 4.3). These are well-established or emerging trends that cover a broad range of misuses for both commercial and non-commercial purposes, including activities that contribute to IP infringement but may not themselves qualify as such. Some of these misuses are specific to social media services, while others occur on other types of services offering similar functionalities. A number of experts pointed to the ability to reach out to social media users based on their interests or those of their social connections as a specific feature of social media that can be exploited by IP infringers in the course of their activities. Experts also identified IP infringers' use of closed and private communication functionalities as an increasingly common method of evading existing IP investigation and protection measures (see Section 4.4). For the purposes of this analysis, trends have been identified separately, but they may be used concurrently by IP infringers in the course of their activities.

4.1 Hosting, streaming or linking to IP-infringing content

As part of their services, some social media services have developed functionalities that are also offered by other types of services, such as file hosting, streaming or livestreaming, and that can be misused to infringe IP.

4.1.1 Hosting and/or embedding IP-infringing digital content

Experts explained that content can be hosted directly by the social media service or simply embedded in social media posts, with full movies and TV series or extracts thereof being made available illegally. They emphasised that short extracts are sometimes considered 'premium content' by rights holders (e.g. a goal during a football match), so the damaging impact of this type of IP infringement should not be underestimated.

4.1.2 Livestreaming sport, TV or other recordings

The development of livestream technology and its integration into social media services was mentioned as facilitating live dissemination of IP-infringing content. Experts highlighted the

development of sophisticated technique to evade enforcement, but also increase illegal revenues, particularly with regard to the livestreaming of certain events (e.g. sports, fashion, movies and TV series releases). This technique involves posting a link in relevant social media interest groups that streams high-value legitimate content in advance of an event, in order to build an audience. The link to this 'innocent' content then turns into an illegal livestream for the duration of the event. This technique minimises the risk of stream or website blocking while maximising IP infringers' advertising revenues. The link to the initial 'innocent' content allows the URL to be classified as safe and valuable, attracting high-value ads even when the content temporarily changes to the illegal livestream of the event.

4.1.3 Linking to IP-infringing content on third-party websites

Experts mentioned IP infringers' use of social media to spread links to infringing content on third-party websites. These links can be shared publicly or through closed groups or private communication functionalities provided by social media services (see Section 4.4), through permanent or ephemeral posts (see Section 5.2.3). According to a Hadopi user survey, the percentage of users accessing IP-infringing content through links found on social media services is higher than that of users accessing infringing content directly on social media ([20]).

4.2 Advertising and marketing IP-infringing services and products through social media

4.2.1 Paid advertising

The display of ads for IP-infringing services or products affects a broad range of legitimate websites and services, including social media. Experts mentioned the use of sponsored advertising by counterfeiters and fraudsters to target consumers with legitimate-looking adverts offering large discounts or low prices as a way to direct social media users to external websites selling counterfeit goods. A similar process is used to direct users to websites offering IP-infringing content, particularly live sporting events.

([20]) Hadopi, Accès illicite à des contenus culturels via les réseaux sociaux (October 2019, French only). According to this survey, 8 % of users access IP-infringing content directly on social media services, and 12 % through links to other websites.

4.2.2 Marketing through social media posts or accounts

Some experts highlighted the practice of simply spreading information on or promoting counterfeit goods and IP-infringing services freely through social media posts or accounts. In some instances, social media influencers actively encourage followers to buy cheap copies of high-end products, accompanying their product reviews with certain hashtags to increase the views of their posts. This trend was considered problematic, as it understates the negative effects of counterfeiting and offers a distorted image of counterfeit goods as trendy or harmless ([21]). One e-commerce marketplace has initiated legal action in a first attempt to address this phenomenon (see Section 6.2.4).

In other instances, operators of IP-infringing services post on the commercial accounts of IP owners to redirect users towards their services. This is particularly true of operators of websites offering infringing film, TV, sport or fashion content trying to redirect followers of the relevant companies towards their own channels. '**Burner accounts**' are frequently used for this purpose, spreading innocent content (e.g. content related to legitimate brands or products) across social media and thereby attracting traffic towards an IP-infringing website ([22]). Some experts highlighted the possibility for IP owners to simply restrict or moderate the content on their official accounts. However, others pointed out that many brands find it difficult to monitor comments posted on their official channels, even with the support of dedicated full-time staff.

Experts also reported the creation of '**scam accounts**', which use well-known brands and trade marks to appear legitimate in order to gather followers, generate traffic towards IP-infringing websites or in extreme cases steal credit card details. This trend, which affects many brands, is supported by the use of '**spambots**' that impersonate users and are capable of autonomous interaction with humans, which promote and spread information on counterfeit goods ([23]).

Some experts argued that as more and more users purchase products online through social media channels, the line between social media platforms and e-commerce has blurred in recent years.

([21]) American Apparel & Footwear Association, Dupe Influencers: The Concerning Trend of Promoting Counterfeit Apparel, Footwear, and Accessories on Social Media, May 2021; Kimiya Shams, We have a problem – influencers endorsing counterfeits (op-ed), *World Trade Mark Review*, 12 April 2021.
([22]) It was explained that the content of the website can be perfectly legitimate in the first place, escaping pre-scanning measures from social media platforms, with the traffic being quickly redirected towards an IP-infringing site or the content changed.
([23]) Andrea Stroppa, Daniele di Stefano and Bernardo Parella, Social Media and luxury goods counterfeit: a growing concern for government, industry and consumers worldwide, May 2016.

Although the rise of social media commerce is bringing about major benefits and new ways to market products and services, it also results in an increase in the fraudulent marketing of counterfeit goods on social media platforms and raises challenges for IP owners and social media services alike ([24]).

4.3 Information on IP-infringing activities

4.3.1 Support forums for IP-infringing services

Experts gave examples of websites, applications and sellers of illicit streaming devices or other actors involved in IP-infringing activities engaging and communicating with their users through social media. Many have 'official' social media accounts that are referred to on their main pages with social media buttons and trackers. These accounts are used to offer general information or news and deal with requests from their users. In some instances, when an IP-infringing website is blocked, the related social media accounts will announce an alternative domain to which users can quickly be redirected.

4.3.2 General information on IP-infringing activities

Experts explained that certain social media groups and pages are used to provide users with general information on IP-infringing activities. Although they may not provide pirated content themselves or link directly to such content, they explain which tools can be used to access it, where to find sources of content, and how to avoid being detected by rights holders or law enforcement services. Some experts also reported the misuse of social media to share explanatory videos showing where to find replicas on major e-commerce marketplaces.

4.4 Closed groups and private communication services

A number of social media services support different levels of communication, allowing users to communicate publicly, with their network(s), in closed groups of users, or privately. Most experts highlighted the combined use of these different levels of communication as a way for IP infringers to evade IP enforcement measures (see Section 5.2).

([24]) This issue was identified, for example, in the American Apparel & Footwear Association's (AFAA) Comments to the USTR on Notorious Markets, 8 November 2020. See also Trevor Little, 'Amazon and Facebook in crosshairs as USTR submissions highlight US platforms', *World Trade Mark Review*, 10 November 2020.

4.4.1 Use of closed groups and chat groups

Many experts highlighted the misuse of closed groups (i.e. invite-only groups) for IP-infringing activities. In some instances, sellers of counterfeit goods use public accounts displaying official brand images or images of authentic products. Users accessing these public accounts are invited to join a specific chat or closed group. These closed groups are used to promote or sell counterfeit goods out of the public eye or to direct users to websites dedicated to such activities ([25]). In other instances, closed groups are misused to exchange links to pirated content. Some of these groups even have paid membership options. The issue of closed groups and the relative safety they provide for IP infringers was also identified in the United Kingdom IPO's 2017 report *Share and share alike* ([26]).

4.4.2 Use of private communication and instant messaging services

Several experts mentioned the use of encrypted communication services to drive social media users towards IP-infringing websites and/or facilitate transactions and payments for IP-infringing products ([27]). In this case, social media's functionalities can be used to promote the IP-infringing service or product, with users invited to contact the seller through the private communication service of the same or a different social media service. A typical example mentioned by one expert is a picture posted on social media including a phone number that can be used to contact the seller through an instant messaging application.

4.4.3 Closed groups pointing to 'hidden' counterfeit offers on e-commerce marketplaces

One expert explained that social media posts in closed groups sometimes link to 'hidden' counterfeit offers on popular e-commerce marketplaces. When a consumer orders, for example, an unbranded shirt or cap on a marketplace using a special predetermined code shared on social media, they actually receive a counterfeit shirt or cap bearing a trade mark. The counterfeit nature of the product is not mentioned and cannot be detected from the marketplace listing itself. This practice seems to

([25]) For example, the AFAA's November 2020 comments to the USTR state that a significant volume of counterfeit goods are being offered to consumers using a range of different methods, including closed groups.
([26]) United Kingdom IPO, Share and share alike: The Challenges from Social Media for Intellectual Property Rights, May 2017.
([27]) This issue is also mentioned in the EUIPO's 2016 report Research on Online Business Models Infringing Intellectual Property Rights, p. 59.

be developing as a way of evading the IP protection measures put in place by some e-commerce marketplaces and/or detection by IP owners through existing monitoring techniques ([28]).

([28]) This issue was also identified in the US Department of Homeland Security's report on Combating Trafficking in Counterfeit and Pirated Goods, January 2019, p. 23.

5 Challenges

There are a number of challenges that affect the ability of IP owners, social media companies and law enforcement authorities to prevent the misuses of social media services for IP-infringing activities, as well as their capacity to cooperate. This discussion paper aims to identify the most relevant challenges that are specific to social media services.

5.1 Regulatory requirements applying to different social media functionalities

Social media services offer a variety of functionalities through which private and business users can share content publicly or communicate privately. Different legal frameworks apply to these different functionalities, and to the different types of content or data held by the social media companies that operate them. This impacts the ability of social media companies to cooperate with IP owners depending on the functionality that is being misused for IP-infringing activities ([29]). This analysis focuses on the EU regulatory framework and does not touch upon specific regulations applying to social media that are emerging in certain Member States ([30]).

In this context, the different social media's functionalities can be divided into two main categories depending on whether the content is available publicly (e.g. to the user's social connections) or through private communication such as instant messaging services. Regardless of the public or private nature of the communication services offered by social media, a different framework applies to the disclosure of the personal data of alleged IP infringers.

5.1.1 Publicly available content

Content-sharing functionalities qualify as information society services, defined as 'any service normally provided for remuneration, at a distance and at the individual request of a recipient of

([29]) In view of the focus of this discussion paper, this section does not cover regulations that may apply to other types of illegal or harmful content such as Directive 2010/13/EU on Audiovisual Media Services or Regulation 2018/640 on terrorist content.

([30]) Regulations applying specifically to social media services have been adopted in Germany (e.g. the Network Enforcement Act adopted on 12 July 2017, the Draft law on combating right-wing extremism passed on 19 February 2020, and the Draft law amending the Network Enforcement Act passed on 1 April 2020) and are under consideration in France (e.g. Article 19 bis of Projet de loi confortant les principes de la République approved by the Parliament on 16 February 2020).

services' ([31]), and are subject to the Directive on electronic commerce ([32]). This includes functionalities allowing users to share user-generated and other creative content, post e-commerce listings or advertise goods and services. Such activities consist in hosting information provided by users and are covered by Article 14 of the Directive on electronic commerce, which states that a hosting provider 'is not liable for the information stored at the request of a recipient of the service' if it 'does not have actual knowledge of the illegal activity or information (…)' and if 'upon obtaining such knowledge or awareness', it 'acts expeditiously to remove or to disable access to the information.'

Since the content is publicly available, social media companies, IP owners and relevant law enforcement authorities can monitor and identify IP-infringing activities occurring on these services. In order to support cooperation with national authorities, Member States and other relevant stakeholders in combating illegal content online, the European Commission has communicated a set of guidelines and principles ([33]) that were further enshrined in the recommendation on measures to effectively tackle illegal content online ([34]).The recommendation proposes a common approach to detecting, removing and preventing the reappearance of illegal content online, while ensuring increased transparency and protection of fundamental rights and freedoms. It urges platforms to adopt 'a clear, easily understandable and sufficiently detailed explanation of their content policy in their terms of service' in order to 'reduce the potential negative effect on the users' fundamental right to freedom of expression and information' ([35]). It also clarifies platforms' liability when taking proactive steps to detect, remove or disable access to illegal content.

The recommendation emphasises the need for clearer **notice and action procedures** for notifying illegal content, including fast-track procedures for 'trusted flaggers' ([36]). Other measures proposed include **IP protection programmes** and **voluntary proactive measures to detect illegal online content** ([37]). ([38]) This discussion paper provides an overview of some of the notification procedures (see Section 6.2.1), proactive measures (see Section 6.2.3) and IP protection programmes (see Section 6.2.2) that have been put in place by social media services.

The proposal for a Digital Services Act

This analysis is based on the applicable European legal framework. However, the European Commission's proposal for a **Digital Services Act** ([39]) (the 'DSA proposal') that applies to all types of illegal content as defined by national or Union law (including IP-infringing content) proposes major changes to this legal framework. The current proposal maintains but clarifies the liability

exemptions that apply to online intermediary services, while reaffirming the prohibition of general monitoring obligations. It proposes a number of due-diligence obligations aimed at supporting the removal of illegal content, while ensuring greater transparency, including on content moderation tools and decisions by online intermediaries.

In addition, social media companies, as intermediaries whose services can be used by third parties to infringe IPRs, can be subject to injunctive relief under EU Directive 2004/48 on the enforcement of intellectual property rights (IPRED) and EU Directive 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society (INFOSOC) ([40]). The relevant authority may order them not only to end the infringement but also to prevent further infringement, irrespective of any liability ([41]).

As for **advertising services**, the European Commission has stressed the need to provide appropriate safeguards, such as 'the use of Content Verification (CV) tools, Ad Delivery and Ad Reporting systems, schedules, online rights monitoring and brand protection services' ([42]).

Furthermore, certain social media functionalities that allow the dissemination of copyright-protected content may also be subject to a special regime under the recently adopted Copyright Directive ([43]).

([31]) Article 1(1)(b) of Directive (EU) 2015/1535 of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.
([32]) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
([33]) European Commission, Tackling Illegal Content Online: Towards an enhanced responsibility of online platforms, 28 September 2017, COM/2017/0555 final, p. 4.
([34]) European Commission, Recommendation on measures to effectively tackle illegal content online, 1 March 2018, C(2018) 1177 final.
([35]) European Commission, Tackling Illegal Content Online: Towards an enhanced responsibility of online platforms, 28 September 2017, COM/2017/0555 final, Section 4.2.1.
([36]) European Commission, op. cit., Section 3.2.1.
([37]) European Commission, op. cit., Section 3.3.1.
([38]) These non-binding measures have been further clarified through the CJUE case law, and in particular in Judgement of 3 October 2019, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, C-18/18, ECLI:EU:C:2019:821 (on defamatory statements).
([39]) Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC.
([40]) Article 9 and Article 11 of IPRED and Article 8(3) of the INFOSOC Directive.
([41]) Commission Communication on Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights, 29 November 2017, COM(2017) 708, p 16 and p. 22 et seq.
([42]) European Commission, 'The Follow the money approach to IPR enforcement – stakeholders' voluntary agreement on online advertising' and IPR Enforcement – Guiding principles.
([43]) Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

5.1.2 Private communication

Private communication functionalities are regulated in a different way. Monitoring and collaborating with IP owners in the context of electronic communication services requires striking a balance between rights and interests, such as the right to privacy and the right to confidentiality of communications. This limits the capacity of social media companies to cooperate with IP owners.

The European regulators and the courts (see table below) have so far been hesitant to declare social media's instant communication services as falling under the definition of electronic communication services and consequently as being subject to the protection regime under Directive 2002/58/EC ([44]) (the 'E-Privacy Directive'), namely the obligation to comply with the principle of confidentiality of communication. This has created uncertainties around the possibility of implementing measures to detect illegal activities, which, in turn, has led to a situation where social media companies, as well as other types of online intermediaries providing such services, refrain from proactive monitoring of services that could be considered private communication services and disclose their content to law enforcement authorities under strict conditions. This approach has been recognised by the European Commission, which noted, however, that the protection of fundamental rights should not be regulated by the industry itself ([45]).

([44]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

([45]) Section 2.3 of Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10 January 2017, COM(2017) 10 final.

The evolving European framework on electronic communication services and e-privacy

Until recently, the communication services provided by social media companies did not in principle fall within the scope of the E-Privacy Directive ([46]). Although there were instances where the Court of Justice of the European Union, after a case-by-case examination, had qualified similar services – regrouped under the notion of 'over the top' or 'OTT' services ([47]) – as electronic communication services ([48]), the situation remained unclear.

However, the European Regulatory Framework evolved further with the entry into force on 21 December 2020 of the European Electronic Communications Code (the 'EECC' – Directive 2018/1972) ([49]), which modernised the definition of electronic communication services. In concrete terms, as of 21 December 2020, services defined as interpersonal communication services classified by BEREC as OTT-0/1 ([50]) are considered electronic communication services and brought under the current E-Privacy Directive. This means that they will now have to apply stricter confidentiality regimes. At the same time, services that do not meet the requirements set out by the EECC, such as blogs or social networks, or services that are a minor or purely ancillary feature to another service, remained excluded ([51]) from the definition of interpersonal communication services.

The application and interpretation of this new legal framework is expected to further clarify whether and to what extent social media messaging services fall under this definition. Clarity is also expected from the E-Privacy Directive, which is, however, currently under revision (the Proposal for a Regulation on Privacy and Electronic Communication). If this regulation is adopted, it could indeed partly include 'OTT' ([52]) services in the category of electronic communication services, even if the communication function does not play a leading role and is an ancillary feature ([53]).

([46]) EPRS, Regulating electronic communications – A level playing field for telecoms and OTTs?, 2016.
([47]) European Parliament, Directorate General for Internal Policies, *Over-the-Top players (OTTs),* Study for the IMCO Committee 2015: 'Over-the-top (OTT) refers to online services which could substitute to some degree for traditional media and telecom services.'
([48]) Judgment of 5 June 2019, C-142/18, Skype Communications, EU:C:2019:460; BEREC, Report on OTT services, BoR (16) 35, January 2016; judgment of 13 June 2019, C-193/18, Google, EU:C:2019:498.
([49]) Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code.
([50]) BEREC, Report on OTT services, op.cit.: 'OTT-0 - OTT voice with possibility to make calls to PATS; OTT-1 - OTT voice, instant messaging'.
([51]) Article 2(5) and Recital 17 of Directive (EU) 2018/1972.
([52]) For example, webmail, instant messaging and computer-based Voice over Internet Protocol services.
([53]) Article 4(2) of the Proposal for a Regulation on Privacy and Electronic Communications, COM(2017) 10 final. See also the Negotiating mandate adopted by the Council of the European Union on 10 February 2021 and the European Parliament report adopted on 20 October 2017.

5.1.3 Access to alleged IP infringers' personal data

In principle, access to data identifying allegedly IP-infringing entities is governed by IPRED. This legislation requires Member States to ensure that in the context of IP infringement proceedings the judicial authority may order the provider of the services used to infringe the IPRs to disclose information regarding, for example, the names and addresses of persons involved in the production or distribution of infringing goods, as long as the claimant's request is justified and proportionate ([54]).

However, when applying this provision, Member States have to ensure that a fair balance is struck between the various fundamental rights involved, including the right of rights holders to information and the right of users to protection of their personal data ([55]). They must also ensure their action complies with other general principles of EU legislation, such as the principle of proportionality ([56]).

Therefore, subject to the above safeguards, social media companies can be ordered to provide certain personal data pertaining to those using their services for IP-infringing activities. In some instances, social media companies have started to cooperate with and are providing investigative support to law enforcement authorities and IP owners as part of joint operations to identify alleged counterfeiters (see Section 6.2.4).

5.2 Use of social media to evade existing measures and investigation techniques

Experts identified a number of challenges involving the evasion of existing IP protection measures and investigation techniques, notably the following.

([54]) Article 8 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (IPRED).

([55]) Judgement of 9 July 2020, C-264/19, Constantin Film Verleih, EU:C:2020:542. In this case, the Court ruled that the concept of 'name and address' under Article 8 of IPRED does not include email addresses, telephone numbers, or IP addresses.

([56]) Judgement of 16 July 2015, C-580/13, Coty Germany, EU:C:2015:485, § 28; Judgement of 9 July 2020, C-264/19, Constantin Film Verleih, EU:C:2020:542; Judgement of 12 April 2012, Bonnier, C-461/10, EU:C:2012:219, § 51-61; Judgement of 29 January 2008, C-275/06, Promusicae, EU:C:2008:54, § 58-59; see also Commission Guidance on certain aspects of IPRED, COM(2017)708, 29 November 2017, p.11.

5.2.1 Combination of different levels of communication

As seen above in Section 4, IP infringers use a combination of social media's public, closed-group, and private communication functionalities to defeat existing IP investigation techniques. According to some experts, this method makes it virtually impossible for IP owners, but also for social media services to detect IP-infringing activities ([57]).

Some experts stated that while some IP infringers were using such advanced techniques, most were using far less elaborate methods, such as posting information concerning their IP-infringing products and services publicly on social media and offering ways to contact them outside the service through chat or private communication services.

5.2.2 Controlling access to closed groups

Some experts mentioned the fact that IP infringers who use closed groups and/or private communications are able to check users' profiles before granting them access to a group or contacting them privately, allowing them to exclude users they suspect of working for IP owners or law enforcement authorities. In that respect, experts noted that not all law enforcement authorities have 'mystery shopper' powers to join such closed groups and establish that infringement has occurred.

5.2.3 Ephemeral content

Experts also mentioned the challenge posed by ephemeral content. The possibility for social media users to create temporary posts (also known as 'stories') that typically disappear after 24 hours allows IP infringers to leave little trace of their activities ([58]). The challenge consists in quickly detecting ephemeral IP-infringing content and having it taken down to limit the harm caused. However, ephemeral content makes it more difficult to identify and prove repeated infringements and suspend or terminate social media services profiles. It also requires monitoring and investigative techniques, allowing to save the IP infringing content, even before it is notified to the social media service, as it may well have disappeared at the time the notice is submitted or processed.

([57]) This trend is not limited to IP-infringing activities. See Europol, How COVID-19-related crime infected Europe during 2020, November 2020, which reports on human traffickers' increasing use of social media groups and instant messaging applications.
([58]) Ghostdata, Instagram and counterfeiting in 2019: new features, old problems, April 2019, p. 10.

Some experts pointed out that ephemeral content presents the same challenge as livestreaming, ([59]) and could in some instances be traced using the same methods. ([60]) They also pointed out that ephemeral content such as 'stories' is not covered by some of the IP protection programmes and tools (see Section 6.2.2) made available to IP owners by some social media services.

5.3 Decentralised social media services

The development of decentralised social media services may present new challenges. Traditional social media services gather information and content from their users that is stored on servers controlled or owned by a single company and managed based on the policies set by this company. In this client-server model, the social media company has control over users' data and accounts and can ensure that content complies with its content policies (on IP protection, for example) ([61]).

Decentralised social networks, by contrast, operate on independently administered servers, building on federated or peer-to-peer (P2P) protocols ([62]) or blockchain technology.

5.3.1 Federated social network

A number of services based on the Fediverse ([63]) take this approach. In this model, any user can set up a server (or 'instance') that implements a specific protocol allowing it to communicate with the rest of the federated network. Each instance only stores its own users' data, but a user signing up with any of the servers has access to the entire network. Each instance can set its own content or moderation policies and block other instances. The Mastodon social network builds on the open-source ActivityPub federated protocol, bringing together more than 4.4 million users ([64]). The challenge with this model is that if servers are run by different individuals or organisations, they can have very different content policies.

([59]) See for instance the 'cloaking effect' as discussed in European Commission, Report on the functioning of the Memorandum of Understanding on online advertising and intellectual property rights, SWD(2020)167 final/2, p. 7.
([60]) For example, automated content recognition technologies.
([61]) Faced with complex decisions around content that may have a significant social impact, some social media companies are exploring new governance and enforcement approaches, including those in which third-party experts make some decisions. This is the case, for example, with the Facebook Oversight Board.
([62]) Decentralized Social Networks: Comparing federated and peer-to-peer protocols.
([63]) https://en.wikipedia.org/wiki/Fediverse.
([64]) As of May 2020. See Mastodon.

5.3.2 P2P protocols

Fully or partly distributed P2P networks allow users to communicate directly with each other without going through dedicated servers ([65]). The challenge posed by this model is that while users can block or ignore content, there is no central moderation of content, and the responsibility falls largely to users.

5.3.3 Blockchain-based social networks

With this approach, users' data and content are stored on a 'blockchain' through a distributed network. This system allows cryptocurrency payments for users supporting the creation or curation of content. Steem service is based on this approach ([66]), and has over a million users. Due to blockchains' limited data-storage capacity, most blockchain-based social networks rely on P2P networks for storing and sharing data in distributed file systems.

Some experts pointed out that decentralised social media services are seeing a growth in their user base and that they have some advantages, in particular when it comes to data protection and users' control over their data ([67]). However, the question of the governance of these services, in particular over hate speech ([68]), fake news and IP protection, is already debated, and these services are likely to pose new challenges for IP owners as they gain in popularity.

([65]) For detailed explanations of different P2P social network protocols, see Ecosystem Review, January 2021.
([66]) Steem, An incentivized, blockchain-based, public content platform, August 2017.
([67]) See the EU-funded project HELIOS, which is 'laying the foundation for a new decentralised social network vision where users take back the control of their data and content, with novel privacy and trust functionalities'.
([68]) Adi Robertson, How the biggest decentralized social network is dealing with its nazi problem, *The Verge*, July 2019.

6 Good practices

A number of good practices already exist or are being developed to address some of the trends and challenges posed by the misuse of social media for IP-infringing activities. This discussion paper does not aim to catalogue all good practices from all players, but rather to establish broad categories of good practices based on concrete examples. Good practices are divided below into preventive and reactive measures in relation to IP-infringing activities.

6.1 Preventive measures

A number of good practices have been developed by social media services to address the issue of IP infringement before any real or attempted infringement occurs on their services.

6.1.1 Terms and conditions and specific policies

Good practices for all types of intermediary services start with terms and conditions. As for social media services, 'terms and conditions', 'community guidelines' and specific policies applying to certain social media functionalities allow these services to define what their users can and cannot do, enabling timely and effective action on the basis of users' contractual (as opposed to legal) obligations.

As an example of good practice, experts highlighted the terms and conditions and specific policies of social media services that make it clear that users should not post IP-infringing content, especially when these terms and conditions are complemented by the following.

- **Information resources** to educate users on the service's policies and procedures, especially with regard to the prohibition of IP infringement. Some experts suggested that this information could usefully link to external resources on IP and practical guidance on how to respect these rights in the context of social media use, as well on the risks of counterfeit goods and the damaging effects of IP-infringing activities in general.

- **Repeat infringer policies** clearly stating the consequences for social media users who repeatedly infringe IP, including the suspension and termination of their accounts, and applying across the service's different functionalities ([69]).

Terms and conditions are central to addressing the different trends identified above (see Section 4). Experts pointed out that different policies may cover different social media functionalities, with some IP infringement-related policies applying only to paid ad services and not to regular posts. They also highlighted the fact that terms and conditions are only effective if they are enforced both proactively and reactively, resulting in the removal of IP-infringing content detected by the service's proactive measures or reported in a notification, and in the disabling of repeat infringers' accounts.

6.1.2 'Know your business customer' (KYBC) requirements and user profile verification

- **Valid identification**: experts mentioned that requiring users to provide valid identification as part of the conditions for setting up a social media account could limit a broad range of IP-infringing uses of social media while facilitating the detection of fraudulent users and repeat infringers. They underlined that authorities and IP owners may need access to valid user identification information in cases of IP infringement.

  Some experts stressed that strong identification requirements at the account creation stage (for example, requiring proof of identity) are hard to implement when no paid services are involved. They also mentioned that the need for users to be identifiable has to be balanced against users' interests, but that there may be solutions to this ([70]) ([71]).

  For example, the violation of Facebook's Community Standards ([72]) against user misrepresentation ([73]) may result in warnings, restriction of the ability to post and, in cases of

([69]) For example, Facebook's repeat infringer policies apply to individual Facebook profiles, Pages, groups and ad accounts.
([70]) For example, it was suggested that a social media user may be required to prove their identity when suspicious activities are detected or notified, with the understanding that these solutions should be fully compliant with applicable data protection regulations.
([71]) Article 22 on the 'traceability of traders', of the initial DSA proposal under discussion in the context of the interinstitutional regulatory process, obliges online platforms to receive, store, make reasonable efforts to assess the reliability of and publish specific information on the traders using their services where these online platforms allow consumers to conclude distance contracts with those traders.
([72]) https://www.facebook.com/communitystandards/introduction.
([73]) See https://www.facebook.com/communitystandards/misrepresentation for information on what Facebook considers to be misrepresentation.

repeated violations, disabling of the user's profile. Where there is a risk of physical harm and/or a threat to public safety, it can also result in law enforcement authorities being notified. With respect to misrepresentation, Facebook has set out a specific 'name policy' ([74]) and has established situations in which an ID document can be requested ([75]), with a list of the types of documents accepted ([76]).

Beyond KYBC requirements and profile verification, some social media services also allow users to report fake profiles ([77]), which can contribute to the identification and termination of profiles that are purposely meant to mislead users into believing that they are official brand or company profiles.

- **Verification of online advertisers' identities**: experts mentioned that some platforms have started to implement broader identity verification requirements for online advertisers to run any kind of online advertisements, in order to provide users with easily accessible information about the advertiser's identity. This information is displayed as a pop-up window beside the advertisement itself ([78]). This good practice has the potential to undermine the use of paid advertising to promote IP-infringing goods and services on social media (see Section 4.2.1).

- **Measures to detect new accounts created by previously banned users and prevent further misuses**: mobile-app based social media services, in particular, can use a combination of the user's mobile phone number and device ID to prevent banned users from opening a new account and continuing to misuse the service ([79]). This good practice undermines the easy circumvention of social media policies against repeat infringers.

- **Measures to undermine the creation of multiple social media accounts**: experts mentioned that some social media services only allow one account to be created per unique email address and limit the number of accounts that can be created from the same IP address

([74]) https://www.facebook.com/help/112146705538576.
([75]) Nevertheless, Facebook does not clearly define when a name confirmation will be requested for situations other than requesting account access.
([76])https://www.facebook.com/help/245465555858336?helpref=popular_topics.
([77]) https://www.linkedin.com/help/linkedin/answer/61664.
([78]) In April 2020 Google launched a policy that requires all advertisers to verify their identities in order to run online advertisements on its platform.
([79]) For example, Weixin (also known as WeChat) states that if an account has been disabled for infringing IP, the mobile phone number attached to the account is permanently blocked.

in a given period. This good practice undermines the rapid or automated creation of 'burner' accounts.

- **Specific requirements to access certain functionalities**: another good practice identified by experts is preventing newly registered users from immediately using certain functionalities, in particular those involving e-commerce or the posting of videos ([80]). This undermines the use of 'burner' accounts and makes it harder for IP infringers to access e-commerce or livestreaming functionalities, as they are required not only to create but also to develop their social media profiles before doing so. This also makes it easier for services to detect profiles that are created for fraudulent purposes.

- **Specific restrictions on using certain keywords in profile names**: experts mentioned that restricting the use of certain keywords in profile names (e.g. well-known trade marks) can limit the creation of profiles for IP-infringing activities. One social media service has developed a database of keywords (including trade marks) that are considered well known in the relevant country or that have been registered as part of its IP protection programme (see Section 6.2.2).

  Any attempt to register a new profile with a name entered in the keyword database is automatically detected, and the system requires the user to provide proof of entitlement before activating the profile. This can include relevant trade mark registration certificate(s), authorisation documents or other supporting documents ([81]). This good practice undermines the possibility for IP infringers to market their activities through profiles that mislead users into believing that they are official brand or company profiles, or to drive traffic to such profiles when a user searches for a given trade mark.

6.1.3 Communication campaigns

- **Campaigns by IP owners**: experts explained that social media can be used to run effective anti-counterfeiting or anti-piracy campaigns. Some companies use their official profiles to run such campaigns, warning users of the risks of counterfeit goods and pointing them towards official distribution channels.

([80]) This is notably the case with Facebook, which does not allow new users to use its Marketplace.
([81]) For example, Weixin (or WeChat) has set up a keyword protection mechanism for the names of its official accounts. See Weixin Report on Protection of Brand Owners, March 2018.

- **Campaigns by social media companies**: some social media companies have developed information resources that provide tips on buying and selling safely on their services ([82]), including specific sections on the prohibition of counterfeit goods, and educating buyers and sellers who show an interest in buying or selling products that are more susceptible to counterfeiting.

  As social media can be misused to provide information on IP-infringing services and activities (see Section 4.3), communication campaigns by IP owners and social media companies can raise awareness among social media users of the risks and damaging effects of these activities. Some experts suggested that collaboration among social media companies, rights holders and law enforcement authorities (in full compliance with applicable data protection laws) could provide insights into the types of users accessing IP-infringing content and help to improve educational campaigns and messages against counterfeiting and piracy.

6.2 Reactive measures

A number of good practices have also been developed by social media services to deal with real or attempted IP infringement after it has occurred on their services.

6.2.1 Notice and action (N&A) mechanisms ([83])

Some social media services have put in place guided N&A mechanisms with dedicated channels for IP owners to report content they believe infringes their rights. These channels feature specialised reporting forms for copyright infringement, trade mark infringement or counterfeiting.

Some experts suggested that the mechanisms offered by some social media services could be better aligned with the more advanced mechanisms made available by some e-commerce marketplaces, in particular as these tend to give IP owners' access to historical records of their notifications ([84]).

([82]) See Facebook, Tips for Buying and Selling Safely on Marketplace.
([83]) The initial DSA proposal, under discussion in the context of the interinstitutional regulatory process looks into notice and action mechanisms for all types of illegal content – see Article 14.
([84]) According to Article 15 (4) of the initial DSA proposal, under discussion in the context of the interinstitutional regulatory process, decisions to remove or disable access to specific items of information provided by the recipient of the service and their justification will be published in a publicly accessible database managed by the European Commission.

Nevertheless, experts consider these mechanisms a good practice, especially when they provide the following features.

- **Information resources for IP owners**: providing clear explanations of who can submit a notice, what information is required, and what additional information, if submitted, can facilitate the removal of allegedly infringing content.

- **Reporting in bulk**: allowing reporting of multiple infringing pieces of content in a single report and across the different functionalities of a social media service (e.g. ads, public content, closed groups, and e-commerce listings).

- **Expeditious process and removal**: some experts explained that on some social media services, content is typically removed within a day, and frequently within a few hours. They stressed the importance of informing IP owners when the content they have reported is removed.

- **Information of users**: when content is removed as the result of an IP owner's notification, including the reason for the removal and the potential consequences of continuing to infringe third-party IPRs, with reference to the service's repeat infringer policy ([85]). The service should also provide an appeal mechanism for users to challenge the removal of their content if they believe it did not infringe IP, and it should reinstate content in a timely fashion following a valid appeal.

- **Verification by IP owners following notification by a user**: experts reported that some social media services allow any user to notify them of IP-infringing content. Content reported by a user as infringing copyright or related to counterfeiting is submitted to the relevant IP owner for verification. The IP owners can then assess whether the reported content actually constitutes an IP infringement and ask for the content to be taken down ([86]). This is considered an efficient way of overcoming the constraints of discovery and identifying infringing content,

([85]) When providers of hosting services decide to remove or disable access to specific information provided by a recipient of the service, the initial DSA proposal, under discussion in the context of the interinstitutional regulatory process, requires that recipients are provided with a statement of the reasons for that decision (Article 15).

([86]) For example, Weixin states that as part of its Brand Protection Platform ('BPP') it links counterfeit information reported by users to IP owners, who can then identify counterfeit goods. Weixin reports that in 2019, it 'sent around 300,000 user reports of infringement leads to brand owners'.

in particular in closed groups or private communication functionalities such as instant messaging (see Section 5.2).

- **Verification of associated content and accounts**: when content is taken down, some social media services use reviewers to look into associated content and/or accounts to determine if these also infringe IP. Such a review may look into content from the same user or group in the form of posts, videos or private group membership. It may lead to the identification of other clearly IP-infringing activities, against which the service can take appropriate action ([87]). Some experts explained that it is common for a single user or group to misuse multiple rights, and that this good practice would allow effective action to be taken against these users and prevent this 'cluster infringement'.

- **Notification of username infringement**: some social media services allow IP owners to report the use of a trade mark in a username ([88]). Given that the mere use of a trade mark in a username does not automatically amount to an infringement, the trade mark owner is required to demonstrate that the username is being used commercially in a confusing or deceptive manner, so that users may be led to believe that the account is affiliated with the trade mark owner's brand.

- **Unified notification forms**: some social media companies that operate multiple social media services use a unified notification form to report IP infringement across their different services ([89]). This reduces the number of notification forms IP owners need to get used to and facilitates notifications.

Some experts also mentioned **good practices by IP owners** when using N&A mechanisms put in place by social media services, including the following.

- **Using existing N&A mechanisms** to report content they have a good faith belief is infringing their IPRs, after verifying that it is indeed unauthorised. A related good practice identified was human review of content notified and of the relevant notifications when IP owners or their

([87]) For example, Weixin states that if its system detects an account related to one used by an IP infringer, this related account is also reviewed together with the account initially detected.
([88]) https://support.snapchat.com/en-US/a/infringement-trademark-username; or https://help.twitter.com/en/forms/authenticity/impersonation#brand_impersonation.
([89]) https://help.twitter.com/forms/trademark.

authorised representatives use automated tools to monitor and report IP-infringing content. In that respect, some social media services provide IP owners or their authorised representatives with feedback on their notifications, including information on how these may be improved to lead to a better resolution ([90]).

- **Providing full information** when following a guided N&A mechanism in a complete and easily digestible way, as well as giving additional information or clarification that may be required by the social media service when following up.

- **Avoiding re-notification** of content that has already been reported and for which complementary information has been requested, or that has been reinstated following a complete and valid appeal process.

6.2.2 IP protection programmes and tools for IP owners

Some social media services have developed IP protection programmes that provide a set of tools to help IP owners identify and report IP-infringing content in a streamlined way.

- **Search and reporting tools**: some social media companies provide tools for searching a subset of the content posted on their services ([91]). One service allows trade mark owners to run a global search, using any keyword, of all its currently active ads, as well the content of its Marketplace or group sale posts. IP-infringing content thus identified can be reported individually or in bulk using the same tool.

  Some experts emphasised that while these tools are welcome, they tend to apply only to certain parts of a social media service's content and functionalities, limiting search and reporting tools to ads and e-commerce listings. They believed that by not allowing searches of individual posts, ephemeral content (e.g. 'stories'), hashtags or usernames, some of these tools are not delivering on their full potential. In particular, they are falling short in addressing some of the trends identified above, such as the use of social media posts or fraudulent brand pages to support IP-infringing activities, as well as the use of ephemeral content. However,

([90]) The initial DSA proposal, under discussion in the context of the interinstitutional regulatory process, contains a provision on notice and action mechanisms listing the information that the notice must contain (Article 14(2)) and obliging the provider of hosting services to inform the notifier of its decision and the possibilities for redress against that decision. (Article 14(5)).
([91]) For an example, see the Facebook Commerce & Ads IP tool application form.

some experts felt this could be a consequence of the application of stricter confidentiality rules to such ephemeral content or individual posts (see Section 5.1.2). In addition, some experts believed that by not allowing searches of all usernames containing a particular name or brand, some tools are making it difficult to address the trend of scam accounts using well-known brands and trade marks to generate traffic towards IP-infringing websites (see Section 4.2).

Experts also mentioned that some social media services do not enable or facilitate the bulk registration of trade marks in their IP protection programmes. Instead, they only allow the registration of one trade mark at a time on a country-by-country basis. The experts suggested that it would be beneficial for some social media services to replicate some of the good practices developed by e-commerce marketplaces in this regard.

- **Reserving or limiting the use of trade mark-related keywords in social media account profiles**: as part of its IP protection programme, one social media service allows trade mark owners to reserve the use of their trade marks in users' profiles names. Upon receipt of a valid document proving the legal ownership of the trade mark in question, the service adds the trade mark to a database of keywords. This is used to detect attempts to register new profiles with these keywords in their names (see Section 6.1.2). This good practice, together with the possibility of reporting the use of trade marks in usernames (see Section 6.2.1), can help to undermine scam accounts that use brands to deceive users and generate traffic (see Section 4.2).

- **Automated content recognition (ACR) systems**: The use of technologies that automatically identify and remove IP-infringing content was highlighted by experts as a good practice.

  Several user-generated content websites and social media services have implemented such technologies. Examples include Facebook's Rights Manager ([92]) and YouTube's Content ID ([93]), which are based on audio, video or livestream fingerprinting and can be used to identify videos posted on their respective services. Participating rights holders can upload reference files into the tool and, when a match is detected, decide what action they want to take. If a rights holder chooses to proactively block videos matching certain criteria, this eliminates the need to submit future notifications, subject to users' ability to dispute blocking action if they

([92]) Facebook, Facebook for media and Updates to Our Brand Safety Controls and Intellectual Property Protection Tools.
([93]) Google, How Content ID works.

have the necessary rights. In this respect, experts mentioned the need for such systems to balance the protection of rights against limitations and exceptions in line with relevant national legislation and Article 17(7) of the Directive on Copyright in the Digital Single Market ([94]).

Some experts highlighted the benefit of granting IP owners' associations access to these tools. For example, in 2019 the Danish Rights Alliance entered into an agreement with Facebook allowing it to use the Rights Manager tool. This enables it to 'to act faster and remove copyrighted content on the platform more effectively' ([95]). The experts also explained that ACR systems are usefully complemented by additional measures to deal more effectively with livestreaming of events (see Section 4.1), particularly the 'trusted notifier' or 'prioritised review' systems that are put in place by some online services.

Some experts mentioned that the development of separate systems by different online services makes it complicated and burdensome for rights holders to submit and update reference files for their content across all the different systems. One 'sector' agreement was mentioned as a good practice in this regard. In 2017, Google and the French anti-piracy group Association de lutte contre la piraterie audiovisuelle (ALPA) signed a partnership agreement under the umbrella of the French Centre national du cinéma et de l'image animée (CNC) ([96]). 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.

6.2.3 Automated detection measures

Experts highlighted good practices by social media services that invest in technologies such as artificial intelligence, including machine learning, and other means to detect, block and reduce the distribution of potentially infringing content on their services ([97]).

([94]) Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.
([95]) RettighedsAlliancen, Annual Report 2019, p. 23.
([96]) ALPA, Presentation Guichet Unique, no date (French only).
([97]) Some experts stated that a recurrent challenge for some of these automated detection measures, which is particularly acute in the European Union, is the difficulty of developing and implementing them in many languages at once.

These automated measures can use a variety of signals to identify relevant content, based on analysis of the content itself and/or the user's account.

- For **ads** or **e-commerce listings**, these measures may involve analysis of the combinations of brand names, keywords, price and discount indicators and other signals typically associated with IP-infringing ads and listings.

- For **video**, measures may involve analysis of key features that are typical of a certain type of content, to trigger a human review to determine whether the content does in fact infringe IP. For example, one expert mentioned technologies that can determine the percentage of green pixels in a livestream, indicating with high probability that it is a stream of a sporting event; a human can then review the content thus identified.

- For **user accounts**, measures may involve the identification of signals, heuristics or behaviours that are typically associated with IP-infringing accounts: for example, an unusually large number of users accessing the content of an account that has only just been created. In this case as well, this is only a signal that triggers a human review to determine whether the user is in fact infringing IP.

Experts mentioned that these measures can best be improved through insights from IP owners and notifications submitted through social media services' own guided N&A mechanisms (see Section 6.2.1). These insights and information provide the data that artificial intelligence systems require to get better at detecting IP-infringing activities and the behaviours typical of IP-infringing users.

Some experts underlined the importance of applying these measures to closed groups, where IP-infringing activities can take place out of the public eye (see Section 4.4), and where social media companies' ability to collaborate with IP owners and law enforcement authorities is limited (see Section 5.1.2). However, it is unclear if closed groups should be considered private communication, and consequently whether automated detection measures can be applied to them ([98]). Some experts

([98]) According to the initial DSA proposal, under discussion in the context of the interinstitutional regulatory process, a provider of a hosting service which disseminates information to the public is considered an 'online platform' (Recital 13). Pursuant to Recital 14, the concept of dissemination to the public 'should exclude dissemination of information within closed groups consisting of a finite number of pre-determined persons'. This recital also clarifies that interpersonal communication services as defined in the EECC, such as emails or private messaging services, fall outside the scope of this Regulation.

also underlined the need for proactive measures to ensure IP-infringing content that has been taken down stays down and is not immediately reposted. In particular, once they have been made aware of an issue by IP owners, social media services can investigate and take action to disrupt activities negatively affecting these owners' business. Some experts mentioned that social media services could replicate good practices developed by e-commerce marketplaces, leading on 'mystery shopper' investigations or collaboration with law enforcement authorities ([99]).

6.2.4 Collaboration with IP owners or public authorities

- **Direct collaboration**: beyond the development of specific tools for collaboration with IP owners, some social media companies also engage directly with IP owners from different sectors. Experts mentioned that such direct collaboration can provide social media companies with relevant insights into IP owners' rights and products, as well as the identification of counterfeit and other infringing goods. These insights can inform and contribute to improving services' anti-infringement activity, from notice and takedown to proactive efforts. However, some experts highlighted an absence of transparent communication and information about such direct collaboration, or opportunities to collaborate, making it difficult to assess its scale or efficiency ([100]).

- **Investigation support**: experts mentioned that social media services can help IP owners and law enforcement authorities to identify administrators of IP-infringing websites who use social media accounts to attract and/or support their users (see Section 4.3). The Aphrodite operations led by Europol and European law enforcement authorities, with the support of different online players, were mentioned in this context. Some social media services already cooperate directly with IP owners and law enforcement authorities in joint operations to seize suspected counterfeit goods and identify the alleged counterfeiters ([101]).

  Some social media companies provide law enforcement authorities with operational guidelines when seeking user records. These information request processes are not always available to

([99]) See, for instance, Direction Générale des Douanes et Droits Indirects, Presentation du plan contrefaçons 2021-2022, February 2021 (French only).
([100]) If adopted in its current form, the initial DSA proposal, under discussion in the context of the interinstitutional regulatory process, could improve such communication and cooperation.
([101]) Weixin reports that in July 2019, its Brand Protection Joint Team, LVMH, and the police forces in China and the United Arab Emirates cooperated in the arrest of 57 suspects, the shutting down of 16 counterfeit workshops and the seizure of over 35 000 infringing products valued at approximately EUR 228 million.

private parties ([102]). For example, Facebook allows law enforcement officials to submit, track and process requests through its Law Enforcement Online Request System ([103]) or through a dedicated mailing address. Similar guidelines and procedures are in place for Instagram ([104]) and Twitter ([105]), while TikTok ([106]) only allows requests by email.

- **Infringing website lists**: Experts underlined that infringing website lists (IWL) can be used to address the issue of social media posts linking to IP-infringing content on third-party websites (see Section 4.1.3), including posts in closed groups.

  There are several types of list. Some are established for informational purposes, encouraging action against infringing websites and raising public awareness of the risks associated with them ([107]). Others are operated either in the context of a 'follow the money' approach or for brand safety purposes, both of them contributing to reducing infringing websites' revenues. The latter type of list is primarily used by advertising and sometimes by payment intermediaries, and is based on voluntary agreements, which may involve public authorities in order to strengthen their legal position or facilitate cooperation. Some of these lists are public, while access to others is restricted to authorised organisations. Some experts suggested that IWLs could also be based on blocking orders issued by courts and public authorities, or on voluntary agreements between rights holders and internet service providers and involving public authorities ([108]). In that respect, they mentioned that social media services can apply IWLs on a voluntary basis to ensure that links to IP-infringing websites are not distributed through their services ([109]).

([102]) Some social media services, such as Facebook and Twitter, have dedicated channels for law enforcement authorities.
([103]) Facebook, Law Enforcement Online Requests.
([104]) Instagram, Information for Law Enforcement.
([105]) Twitter, Guidelines for law enforcement.
([106]) TikTok, Law Enforcement Data Request Guidelines.
([107]) European Commission, Counterfeit and Piracy Watch List, December 2020; or USTR, 2020 Review of Notorious Markets for Counterfeiting and Piracy, January 2021.
([108]) See, for example, the modus operandi of the German Clearingstelle Urheberrecht im Internet (CUII) (German only) launched in March 2021. Ernesto Van der Sar, ISPs and Rightsholders Unite to Block Pirate Sites in Germany, *TorrentFreak*, March 2021.
([109]) Beyond the removal of links to infringing sites, some experts also suggested that social media services could proactively block outbound links in order to disable the linking at the source.

In Denmark, the Ministry of Culture has fostered these voluntary practices among advertising companies and payment providers and is now looking into extending them to social media services ([110]).

Some experts mentioned the WIPO Alert database ([111]), a secure online platform hosted by the World Intellectual Property Organization (WIPO), which makes national IWLs available to the advertising industry. The aim is to use this information to avoid placing advertisements on infringing websites. Under this scheme, access to the list is strictly regulated, chiefly for reasons of data protection; the national authority creating such a list remains solely responsible for its content. Some experts suggested that these databases should be opened to other intermediaries.

- **Legal action against users**: in a first attempt to deal with the problem of social media influencers actively promoting listings for counterfeit goods on its service, one e-commerce marketplace has started initiating lawsuits against individuals, including influencers ([112]). Some experts suggested that beyond taking measures against users on the basis of their terms and conditions ([113]), legal action by social media companies against influencers exploiting their audience to promote IP-infringing products or services may also constitute a good practice (see Section 4.2.2).

([110]) RettighedsAlliancen, Annual Report 2018, p. 6, and Annual Report 2019, p 15.
([111]) WIPO, WIPO ALERT. Certain EU Member States, such as Spain and Italy (the latter via Autorità per le Garanzie nelle Comunicazioni - AGCOM), are already uploading IWLs on this platform, which is meant to address the problem of online piracy.
([112]) Trevor Little, Amazon sues influencers over fakes, renews call for social media companies to step up, *World Trade Mark Review*, 13 November 2020.
([113]) For another example of a lawsuit filed against an individual user for a breach of a service's terms and conditions and a trade mark owner's IPRs, see Jessica Romero, Facebook and Gucci File Joint Lawsuit Against International Counterfeiter, *Facebook Newsroom*, 26 April 2021.

7 Conclusion

Experts have identified a broad range of trends in the misuse of social media functionalities for IP-infringing activities. Some of these trends are not exclusive to social media but affect other services offering similar functionalities, such as advertising or e-commerce. Other trends are limited to social media, with IP infringers:

- leveraging social media functionalities to target and build an audience and market their goods and services through public posts or in closed groups;

- using specific functionalities to evade existing IP protection measures and investigation techniques, in particular through the use of closed groups and ephemeral content.

Some social media services have developed preventive and/or reactive good practices to address different misuses of their services. From this discussion paper it appears that:

- Some good practices are meant to address the misuse of generic social media functionalities enabling users to share content publicly (e.g. notice and take down or measures to prevent repeat infringers) and are relevant to most social media services.

- Some are more focused on specific business-related functionalities, such as ads or e-commerce functionalities (e.g. IP protection programmes), or are dedicated to a given content format (e.g. text, video, or audio), and are only relevant to social media services offering these functionalities.

- Only a small number of good practices address the misuse of social media's private communication functionalities, or the use of closed group channels to evade traditional IP investigative techniques. This may be partly explained by the legal framework that applies to these functionalities and limits social media companies' ability to cooperate with IP owners and law enforcement authorities. However, this only underscores the importance of some of the good practices that can undermine these trends, including user notifications and infringing website lists.

Finally, all the good practices identified have been developed with traditional social media in mind. The rise of decentralised social media may well pose a number of new challenges and issues that will need to be carefully monitored in the future.

SOCIAL MEDIA – DISCUSSION PAPER

New and existing trends in using social media for IP infringement activities and good practices to address them

ISBN – 978-92-9156-296-1