EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

APPS & APP STORES

Challenges and good practices to prevent the use of apps and app stores for IP infringement activities

July 2024

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, in order to continue deepening its understanding of the trends and challenges in the field of apps and app stores, as well as of the good practices to address it. This discussion paper may be subject to reviews or updates based on any further input from experts or new developments in the field.

APPS AND APP STORES – DISCUSSION PAPER

Catalogue number: TB-05-24-469-EN-N ISBN: 978-92-9156-358-6 DOI: 10.2814/788692

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-infringing activities, and how these misuses can be counteracted through good practices. Having looked at automated content recognition ([1]), domain names ([2]), social media ([3]), payments ([4]), transport and logistics ([5]) and live event piracy ([6]), this seventh discussion paper examines apps and app stores. It aims to contribute to a better understanding of how apps and app stores are misused to infringe IP or support IP-infringing activities, the challenges raised by this misuse, and existing and developing good practices through which they can be addressed.

([1]) Automated Content Recognition – Phase 1 Discussion Paper: Existing technologies and their impact on IP, EUIPO, 2020. Automated Content Recognition – Phase 2 Discussion Paper: IP Enforcement and management use cases, EUIPO September 2022.
([2]) Domain Names – Discussion Paper: Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP infringement activities, EUIPO, 2021.
([3]) Social Media – Discussion Paper: New and existing trends in using social media for IP infringement activities and good practices to address them, EUIPO, 2021.
([4]) Payment – Discussion Paper: Challenges and good practices for electronic payment services to prevent the use of their services for intellectual property-infringing activities, EUIPO, 2021.
([5]) Transport and Logistics – Discussion Paper: Challenges and good practices for transport and logistic services to prevent the use of their services for IP-infringing activities, EUIPO, 2022.
([6]) Live Event Piracy – Discussion Paper: Challenges and good practices from online intermediaries to prevent the use of their services for live event piracy, EUIPO, 2023.

Executive Summary

The number and use of apps has been increasing over the past 15 years. They have become a major channel for users to access content and a broad diversity of services from e-commerce to banking. They support access to content and services through multiple devices, from mobile phones and tablets to TV displays and smart watches.

Apps are typically distributed through app stores, particularly the two stores provided by major operating systems, although users can also find and download apps from app stores provided by specific device manufacturers and other third parties. In some instances, they can also be downloaded and installed outside of any app store like any other type of software.

The increased use of apps and app stores have brought about many benefits for consumers and businesses but has also led to their misuse for illegal and fraudulent activities, including IP-infringing activities. The paper identifies several categories of IP-infringing activities, including:

- **infringement of the IP rights on legitimate apps**, where apps or specific parts thereof are being illegally replicated or copied;
- **infringement of third-party IP rights through apps**, including the illegal use of trade marks and/or logos to mislead users into installing fraudulent apps, or apps used to distribute pirated content and counterfeit products;
- **legitimate apps supporting IP-infringing activities**, such as private communication apps used to share information and instructions on ways to access pirated content or purchase counterfeit products.

Such IP-infringing activities do not only harm right holders as in some instances they are also used to defraud users and advertisers including:

- **spyware,** spread through piracy apps or apps impersonating a legitimate brand, transmitting personal data of the device and users without the user's notice and consent;
- **ad placement fraud**, with advertisers being misled into placing advertisements on fake apps in the mistaken belief that they are legitimate or belong to a respected brand, when instead they have been cloned or squatted.

IP infringers are deploying different techniques to evade detection from app stores and right holders and subsequent enforcement including:

- **apps being disguised** as games or other seemingly legitimate apps to hide their illegal purpose;
- **apps hiding malicious code from app store reviewers** through encryption or delay, with additional code being installed only after the initial installation or through updates;
- **piracy apps with integrated Virtual Private Network (VPN)** for their users to hide their IP address and circumvent blocking measures or geolocation-based content access restrictions.

Experts contributing to the discussion paper identified a number of challenges to counteract the misuse of apps and app stores in the context of IP-infringing activities, including the following.

- **Detection**: different methods must be used depending on the functionality of the app, the infringing activity and where the app can be found. In particular, IP right holders may need to use specific hardware and software to install and inspect the app to determine its IP-infringing nature.
- **Enforcement**: although app stores have terms and conditions detailing the information a developer must provide to upload apps, infringers are still managing to use misleading or fake contact details. This also applies to the information the developer provides about the app's functionality or purpose, which sometimes lead to delayed decisions about blocking or removal of the app from the app store. Moreover, experts also explained that even if an app is removed from an app store it stays on the users' devices and can still be used.

The drafting of this discussion paper took place before the full application of the Digital Service Act (DSA) on 17 February 2024. In that respect, the Observatory and its experts worked on the understanding that some of the current good practices identified in this discussion paper would turn

into regulatory obligations or may need to be adapted to ensure compliance with this new EU regulation.

Experts identified existing good practices from some app stores, right holders and law enforcement authorities to counteract the misuse of apps for IP-infringing activities, including the following.

- **App stores developer agreements and policies**: setting up general provisions regarding the requirements an app needs to fulfil, including on IP-related issues. They also include sanctions that a developer can face if they do not comply, such as removal and/or suspension of the app and, in some cases, even termination of their developer account.

- **User and app verification**: with personal information that a developer needs to provide in order to setup a developer account and, subsequently, what information is required for the app itself, as well as various checks that are performed by some app stores in their review of apps accepted on their platforms.

- **Notice and action mechanisms including automated alerts**: provisions on what is required to submit a notice to have an app removed from app stores, including some stores actively notifying users once an app has been deleted from their store.

- **Cooperation between IP rights holders, law enforcement authorities and member associations**: with initiatives in the form of creating tools, memorandum of understandings, joint task forces and targeted operations.

This discussion paper will hopefully contribute to a better understanding of the different actors and their respective roles in the app ecosystem and of the challenges to counteract the misuse of apps and app stores for IP-infringing activities. By identifying good practices to address such a misuses, it should also further the understanding on ways to address such a misuses, keeping in mind that good practices identified may turn into regulatory obligations or need to be adapted to ensure compliance with new EU regulations, starting with the Digital Service Act.

Table of Contents

1 Introduction and background

1.1 Misuse of apps and app stores for IP infringement activities

Back in 2010, as the number and usage of apps started rising, two journalists ([7]) predicted the decline of the Web to be taken over by 'platforms that use the Internet for transport but not the browser for display'. Although their prediction on the death of the Web did not materialise, the prediction on how people would increasingly access information and services through apps was correct.

The rise of these software solutions designed for a particular purpose is driven by multiple factors.

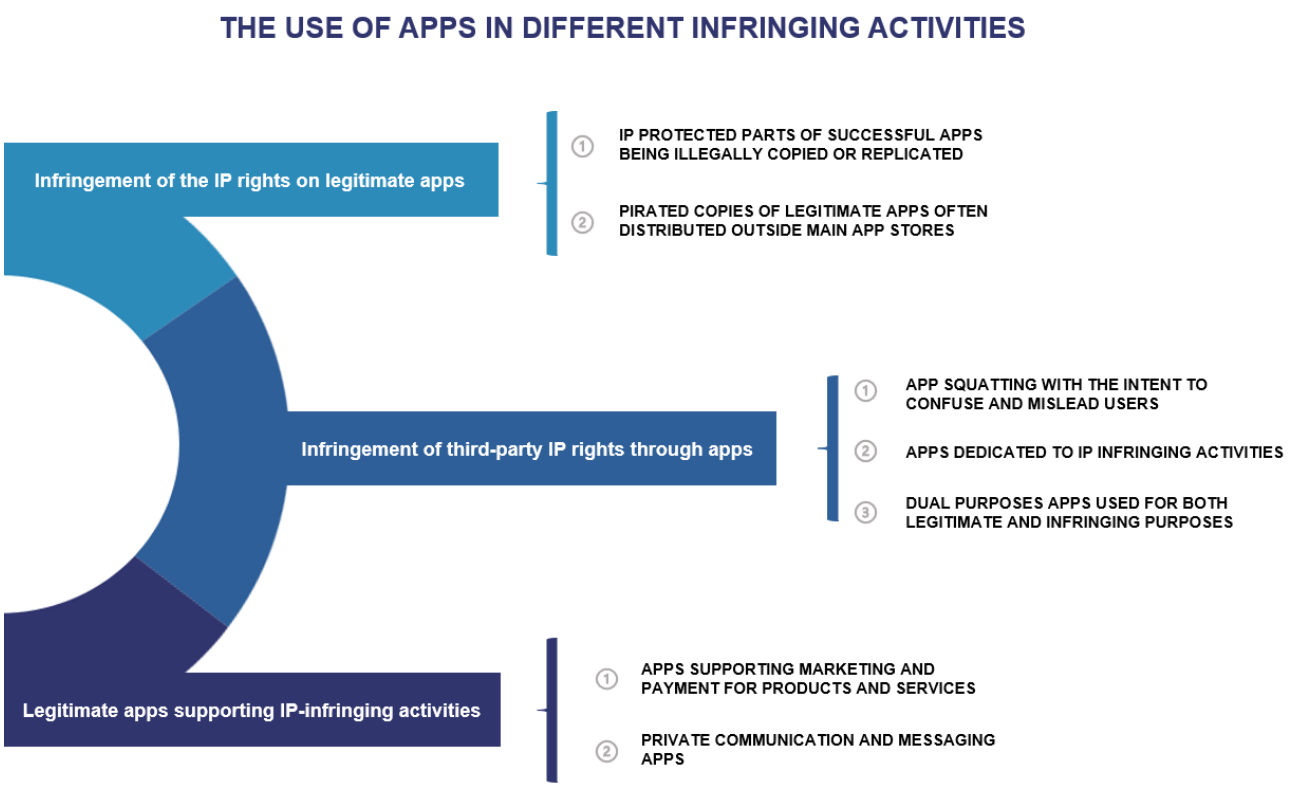
- The **surge in mobile phone usage**, with 7.26 billion mobile users globally in 2022 ([8]) and around 255 billion mobile apps ([9]) downloaded in the same year ([10]).
- The **diversity of connected devices on which apps can be installed**, starting with mobile phones and tablets, but also smart TVs, smart watches, video games consoles and Internet of Things (IOT) devices.
- The **diversity and increasingly sophisticated services delivered through apps**. Although apps were initially performing basic functions (e.g. managing contacts or listening to music), they are becoming central to many of users' daily life activities such as media consumption, shopping, communication, banking or transport.
- The **simplicity and convenience to find and use apps**, with app stores allowing users to easily search and install apps that suit their needs on all type of devices, including computers.
- Better **user experience** when using apps on mobile devices with touch screen rather than when accessing web content (e.g. with personal computers).
- The **new category of internet users**, the mobile only population that only have a mobile subscription and no fixed broadband subscription ([11]).

Apps are typically distributed through app stores, including those provided on major operating systems (e.g. Google Play that runs on Android OS, or Apple App Store for devices enabled by Apple operating systems), mobile device manufacturers (e.g. Samsung or Huawei provide their own

([7]) 'The Web is Dead. Long Live the Internet', 2010, retrieved from Wired Magazine.
([8]) 'Forecast number of mobile users worldwide from 2020 to 2025 (in billions)', 2021, retrieved from Statista.
([9]) Type of application software designed to run on a mobile device, such as a smartphone or tablet computer. See the complete definition of 'Mobile Application' at Techopedia.
([10]) 'Number of mobile app downloads worldwide from 2016 to 2022 (in billions)', 2023, retrieved from Statista.
([11]) 'The App Economy in the European Union', 2020. p.21 and p.26, retrieved from Deloitte.

app stores on their devices), as well as app stores provided on other devices such as smart TVs, e-readers, video game consoles or computers. Furthermore, there are other actors that do not develop or adapt existing operating systems for devices but provide generic third-party app store services. This type of store usually provides apps for devices that run various operating systems ([12]) and can be installed on the device. In addition, for most devices, software and apps can also be sideloaded, (i.e. downloaded and installed as a stand-alone file outside of an app store) ([13]).

Although apps and app stores are bringing about major benefits for consumers and businesses, they can also be misused in the context of illegal and fraudulent activities, including IP infringements or dissemination of malware, just like any other software. This leads to a situation where apps are used in different ways as part of IP-infringing activities:



([12]) E.g. Android OS, Windows.
([13]) See the complete definition at Cambridge English Dictionary. Cambridge University Press, [n.d.]. from https://dictionary.cambridge.org/dictionary/english/sideloading. Last accessed on 19 February 2024.

- **Infringement of the IP rights on legitimate apps**: just like other types of software, apps can be illegally copied in part or in full in the following ways.

    - **Pirated copies of legitimate apps** are often distributed outside of the main app stores and are often used to spread malware or adware ([14]).
    - **IP protected parts of successful apps** (e.g. code, users' interface or functionalities) can be illegally copied or replicated. In some instances, IP infringers are building on such successful components of existing apps to design apps used to spread malware or adware.

- **Infringement of third-party IP rights through apps**: third-party IP rights can be infringed through apps in the following ways.

    - **App squatting** with apps using the protected name and/or visuals of a company to confuse users into believing the app is from this company. Similar to cybersquatting, this can be used to mislead users and drive traffic to apps used for fraud, malware or IP-infringing activities.
    - **Apps dedicated to IP-infringing activities** and, in particular, apps used to provide access to pirated content or marketplaces selling counterfeit products.
    - **Dual purpose apps**, with apps that can have a perfectly legitimate use but are mainly or exclusively used for IP-infringing purposes. This is, for example, the case for certain media players or e-commerce apps, which can be difficult to distinguish from similar legitimate apps, supporting IP-infringing activities.

- **Legitimate apps supporting IP-infringing activities**: as a growing number of services are provided through apps, they are misused by IP infringers in the course of their illegal activities, including:

    - **apps supporting marketing and payment for goods and services**, for example second-hand marketplaces, social media or payment apps;
    - **private communication and messaging apps** that are misused as part of IP-infringing activities to provide information, support or finalised transactions.

([14]) See definition in TechTarget. Last accessed on 25 March 2024.

In addition to the harm to IP right holders, the business models of a number of IP-infringing apps also consist of spreading malware that may also harm the users in different ways depending on the purpose of that malware ([15]).

1.2 Background and objectives

In this context, the European Observatory on infringements of Intellectual Property Rights of the EUIPO ('the Observatory') presented a new workstream to the Expert Group on Cooperation with Intermediaries (Expert Group) to explore how apps and app stores are being misused as part of IP-infringing activities. The Observatory asked the Expert Group to help further the understanding of the app and app store ecosystem, and of the existing good practices to address IP-infringing activities. Therefore, the aims of this analysis are as follows.

- **Map the entire app and app store ecosystem**, which is comprised of a complex web of players, including operating systems developers, device manufacturers, developers of app stores and apps. The objective is to further the understanding on the respective roles, interplay and levels of control of the different players in the ecosystem.

- **Identify trends and challenges**, focusing the analysis on infringement of third-party IP rights through apps, as well as the strategies developed by IP infringers to escape IP-infringement measures from app stores, IP right holders and law enforcement authorities.

- **Identify and analyse good practices** put in place by app stores or specific apps to limit the misuse of their services for IP-infringing purposes and, in particular, voluntary solutions as well as cooperation with IP owners and/or public authorities.

1.3 Scope of the discussion paper

This discussion paper mainly focuses on IP-infringing activities directly affecting third-party IP rights through apps. Although the use of a number of **legitimate apps** (e.g. social media, e-commerce, communication, payment) in support of IP-infringing activities is mentioned, this is not the main focus

([15]) E.g. ENISA Threat Landscape 2020 – Malware, p. 8 ENISA, 2020.

of the paper. As described in Section 2.1, the development of the app ecosystem has led to a situation where many social media, e-commerce or payment website-based services are now also available through apps. Several discussion papers have already analysed how such services can be misused in the context of IP-infringing activities, so this discussion paper only analyses the specificities of the misuse of such services in the form of apps.

In addition to apps, there are also **web applications** that reside and run on remote servers and can be accessed online through a web browser. While experts agreed that this type of applications may raise issues, they point to their limited market adoption and functionalities, and agreed that they could be kept outside of the scope of the analysis and analysed at a later stage.

The drafting of this discussion paper took place before the full application of the Digital Service Act (DSA) ([16]), on 17 February 2024 and the Digital Markets Act (DMA) ([17]), on 2 May 2023. In that respect, the Observatory and its experts worked on the understanding that some of the current functioning of app stores and the good practices identified in this discussion paper would turn into regulatory obligations or may need to be adapted in order to ensure compliance with the DSA and DMA. Experts agreed that it would still be useful to analyse these good practices, while mentioning the specific provisions of the DSA which affects them.

Furthermore, the implementation of the DMA is expected to lead to the introduction of additional distribution channels for apps, which, in combination with the implementation of the DSA, could increase competition between app stores but also app developers. For example, it could enable providers of alternative app stores to compete with the app review processes of designated gatekeepers ([18]) or very large online providers ([19]) under the DMA/DSA, including in ensuring that their level of protection of the intellectual property rights (among other aspects such as security) may be higher than that of the gatekeepers' app stores.

([16]) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).
([17]) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).
([18]) See Article 3 p.1 and 2 in Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).
([19]) See Article 33 p. 4 in Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

This discussion paper complements the work led by the Observatory on the use of apps for IP infringements on a commercial scale and focuses more on how criminals generate revenue from this misuse. It also looks at different investigation techniques to detect and act against infringers. This study (Research on Business Models Infringing Intellectual Property Phase 6: Applications Related to Serious and Organised Intellectual Property Crime, EUIPO, 2024), which is published together with the discussion paper, forms part of a commissioned series of studies investigating business models used to infringe intellectual property rights (IPRs).

2 Mapping of the app and app store ecosystem

2.1 Evolution of the apps landscape

With the rise in mobile phone usage and the development of mobile and other smart devices, users can today use apps for almost everything they want to do online.

2.1.1 Spreading of apps across connected devices

Although the first app was created in the 1980s for the 'World's First Practical Pocket Computer' ([20]), it was not until 1993 and the first smart phone that apps like the ones accessible today gained popularity ([21]). At that time, a phone came with built-in apps providing basic functions such as calculation, checking the date and managing contacts.

Modern smart phones and other smart devices supporting apps did not really exist in their current format until 2002 when BlackBerry released its first phone that supported wireless email ([22]). After 2002 the development moved quickly, with several companies introducing their own smart device solution and with the first iPhone being introduced to the market in 2007, followed a year later by the Apple App Store together with Google's Android operating system and Android Market. 2008 also saw HTC release its first Linux-based Android smartphone ([23]).

Although the Apple App Store initially only had around 500 apps, in 2009 they exceeded 1 billion downloads, with Android Market reaching similar figures in 2010 ([24]). In the following years, the number of downloads of apps rose exponentially, building on the release of new connected devices.

The first apps were fairly basic and performed only one task such as calculating or sending messages, although apps quickly developed to perform several complex tasks. A number of companies created apps that provided all their services in order to become 'go-to-apps' ([25]) for the

([20]) 'Psion Organiser 1', retrieved from Computing History UK.
([21]) 'Tracing the History and Evolution of Mobile Apps', 2015, retrieved from Tech.co.
([22]) 'A Complete Evolution of Mobile and Mobile Apps', 2024, retrieved from ColorWhistle.
([23]) Ibid.
([24]) Ibid.
([25]) 'A Brief History of Mobile Apps', 2021, retrieved from Capitol Technology University.

user. Apps quickly became a new and complementary way for a number of web-based services (e.g. e-commerce, media, banking) to provide these services on their users' connected devices.

In the media sector, apps' faculty to accommodate different business models, while supporting end users' access to content across multiple devices, made them a central element of audiovisual and news content distribution. Mobile games also grew in importance and revenues for the video game sector, accounting for 51 % of the global market in 2022. In the European Market, mobile games account for more than half of the market at EUR 12.31 billion ([26]). Other actors such as social media platforms and streaming services have expanded their offerings by introducing mobile games into their services ([27]), which contributed to the revenue growth of some mobile game providers ([28]).

Apps also became a new and complementary way for brands to engage with their customers in new and interactive ways (e.g. retail apps providing rewards or discounts, luxury brand apps providing exclusive offers or content).

With **apps becoming an important element of several online services and brand engagement strategies**, app store consumers' spend grew to USD 171 billion in 2023, with users spending more than 5 hours a day on apps, and shopping apps totalling over 100 billion hours use over the same year. A staggering 257 billion new apps were downloaded in 2023, which represents 489 000 apps downloaded per minute ([29]).

In parallel, **apps expanded outside of the smart phone sector to reach all connected devices, including TV sets**, with TV manufactures' built-in operating systems allowing users to access apps. Modern smart TV sets now allow users to download apps from an app store (either the manufacturers' or third-party app stores) and build on top of smart TVs functionalities like spatial gesture input and speech recognition. Apps can also be used on TV sets using a range of devices that plug into the screen including PCs, gaming consoles, HDMI dongles or similar devices/boxes. Apps have further developed to be the primary way for users to access all types of services and functionalities on all connected devices from smart watches and voice assistants to connected cars.

([26]) 'Commission Staff Working Document – European Media Industry Outlook', 2023. 150 final, p.55, retrieved from European Commission.
([27]) 'New Entrants tap into gaming for engagement and retention', 2024, retrieved from VCCafe.com.
([28]) Experts have pointed to games like Farmville that has become hugely popular on app stores provided from within social media sites like Facebook.
([29]) 'State of Mobile 2024 – The Industry's Leading Report', 2024, retrieved from data.ai.

Recent years have also seen the development of '**super-apps**', which, in most instances are services that develop as apps from the start to encompass a growing number of functionalities (e.g. e-commerce, payment, delivery, transport, communication, social network), providing a one-stop-shop for multiple personal and commercial services. These 'super-apps' (e.g. WeChat or Line) usually build on top of core features (e.g. messaging, e-commerce and payment), while giving access to independently developed '**mini-apps**' that allow for integration of other services. These types of 'super-apps' are mainly developed and used in Asia, however some 'light' super-apps are developing in Europe ([30]).

2.1.2 Developer landscape

As explained above, an app is like any type of software that can be installed and run on a device, for example, a smartphone or tablet ([31]). Although the first generation of apps were built using basic programming languages, today's apps are built using specific tools and technical skillsets.

The developer decides what type of app to develop and what functionality it should have. There are certain requirements that need to be fulfilled depending on where the app will be offered. Most app stores have terms and conditions that define what is needed from the developers to be able to upload an app to the specific store. This includes, inter alia, software requirements, payment information, developer information and adherence to content policies (see Section 4).

Apple's iOS and Google's Android are the two primary platforms for mobile apps. Apps can be developed using **Software Development Kits** (SDKs) ([32]). These kits are usually created for specific hardware and software platforms (native) ([33]) and therefore the app using an SDK for a specific device or operating system will only work on that specific device or operating system. The developers in these cases must decide where they want to publish their app and for what type of devices and operating systems. If they want their app to be offered on different operating systems, they usually have to create further versions of the same app. However, solutions have been developed to support the creation of apps that are adapted for several operating systems (e.g. operating systems on Apple devices, such as iOS and operating systems of Android OS enabled devices), 'cross-platform mobile

([30]) 'Will Europe get a superapp, and who will it be?', 2022, retrieved from Sifted.
([31]) See the definition of 'Mobile Application', retrieved from Techopedia.
([32]) See 'SDK versus API: What's the difference?', 13 July 2021, IBM.
([33]) iOS SDK for Apple and Android SDK for Android.

development' ([34]). This process allows the developer to create one app that will function on several operating systems. This approach to app development saves time for the developer and allows them to reach a wider user base. However, since they are limited to features that are shared by these operating systems, their features libraries are normally smaller, and the app's performance is usually less optimised.

SDKs like those provided by the main platforms include code libraries (frameworks), which offer shortcuts to code sequences repeatedly used by programmers and which provide a wide variety of readily available functionalities. These functionalities can be complemented by including additional **SDKs and code libraries made available by other providers to offer specific and/or additional functionalities such as analytics, advertising and payment** in an app ([35]). The additional functionalities are directly included in the code of the app and may make access to the services offered by third-party providers easier. For example, apps monetised through advertising typically serve ads by integrating code from **ad-tech companies' SDKs**. This facilitates the implementation of ads for the app developer, while providing the ad-tech company with signals to display relevant ads (e.g. user's location, device type and operating system).

Although app development requires computer programming skills, in recent years tools called app builders or platforms have been developed, enabling people with limited technical skills to develop apps through graphical users' interfaces and configuration ([36]). Some experts explained that the security standards of these apps are typically lower and may raise security issues for their users.

2.2 Different sources of apps

Apps are typically pre-installed on the device or downloaded from an app store. In addition, apps can be downloaded and installed outside app stores, also called 'sideloading' (see Section 2.2.2).

([34]) 'What is cross-platform mobile development?', 27 October 2023, retrieved from Kotin.
([35]) Some third-party SDKs are for example listed in the Google Play SDK index.
([36]) E.g. Top App Builders (2024), retrieved from Business of Apps.

2.2.1 App stores

Since app stores act like a storefront that allow search, download and review of apps, this is generally where users search and find them. App stores typically have processes in place to approve apps before they are offered on their stores. This can include checking specific technical requirements and compliance of the app with the app store terms and conditions (see Section 4).

2.2.1.1. Operating systems

The two major operating systems for mobile devices are Apple's iOS and Android ([37]). Each have their own dedicated app store.

Apple App Store: Apple devices use the iOS operating system and come with certain pre-installed apps, including the Apple App Store App. At the moment, this is also the only app store ([38]) allowed on such devices ([39]) and all apps must be downloaded through it. The apps found on the Apple App Store are developed using developer kits ([40]) specifically adapted to that operating system and can only be uploaded and offered on Apple App Store ([41]). However, Apple allows certain developers to offer apps for internal use by the employees of their company. These apps do not go through the normal review process put in place by the Apple App Store and will be cancelled if offered to anyone outside the company ([42]).

The Apple App Store has extensive terms and conditions for developers and companies that want to publish an app on their store ([43]), including obligations not to use their software for any illegal purposes and that the apps do not contain any malware and/or other harmful code. In addition, the terms and conditions contain information on the review process preceding the publication of an app and the obligations applying to a developer. This includes checking the content of the app and re-submission of the app if any modifications are done before, during and after its publication ([44]). A

([37]) Android is an open-source software and developed by a consortium called Open Handset Alliance. However, the most used version of Android is developed by Google. For more information, see information retrieved from Statista.
([38]) As mentioned, this will change after the full application of the DMA. The DMA will also influence the rules about payment and commissions. Apple has already implemented certain changes, see Update on apps distributed in the European Union - Support - Apple Developer, last accessed on 28 March 2024.
([39]) See also Section 3.2.2. of Apple Developer Program License Agreement.
([40]) For more information on iOS SDK, see Apple Developer.
([41]) See Section 7.6. of Apple Developer Program License Agreement.
([42]) For more information, see Apple Developer Enterprise Program.
([43]) For more information, see Apple Developer Program License Agreement.
([44]) For more information, see Apple Developer Program License Agreement, Section 6.

developer must pay an annual fee ([45]) and, depending on the app's business model and functions, commission ([46]) on apps and all purchases made through it ([47]).

Google Play: apps for Android OS are also developed using specific developer kits ([48]) and can be offered on Google Play and alternative apps stores. Google Play has extensive contractual obligations ([49]) that developers need to comply with, including several policies that cover a broad range of issues ([50]). These include obligations on not violating third parties' intellectual property and spreading malware. In addition, Google Play has a review process in place before an app gets published ([51]). Google Play charges developers a one-time fee ([52]) to be able to publish apps on their store. Depending on the app's business model and functions it also charges commission on apps and purchases made through it ([53]).

2.2.1.2. Devices

The nature of the Android OS allows other app stores to be pre-installed on devices using it – typically the stores of the device manufacturer – or be installed by devices' users. Several device manufacturers ([54]) have created their own dedicated app stores that they preload on their devices. These stores typically have a more limited and/or curated selection of apps. Some of these types of apps are developed by and/or with the device manufacturers' permission. The stores also have terms and conditions that need to be followed with similar obligations to those of the Apple and Google stores ([55]) but can sometimes exclude fees for uploading of apps.

There are also stores that are more specialised to one device and its functionality, such as the Microsoft Store on Xbox ([56]). Although a limited number of mainstream music or video apps can be downloaded (e.g. Netflix, Spotify) from such a specialised store, this store mainly supports the downloading of video games and certain audiovisual services for its users due to the nature of the

([45]) For more information, see Apple Developer Program License Agreement, Section 8.
([46]) See section 3.4. of Apple Developer Program License Agreement.
([47]) Although see footnote 38.
([48]) For example, Android Developer or Google Android SDK.
([49]) See Google Play Developer Distribution Agreement.
([50]) See Google Play policy center.
([51]) See App review process and requirements for the Google Workspace Marketplace.
([52]) See How to register for a Google Play Developer account.
([53]) See Google Service fees.
([54]) E.g. Samsung and LG, as well as Amazon with its app store available on its fire devices (e.g. Fire Stick).
([55]) E.g. Galaxy Store App Distribution Guide.
([56]) See Microsoft Store on Xbox.

device. Similar to other app stores, it does have terms and conditions that impose obligations on its developers to which they must adhere (see more under Section 4.1).

2.2.1.3. Third-party stores

There are several app stores that offer apps to users of devices running on Android, which are not connected to a specific device manufacturer. Companies such as Amazon, Baidu or Tencent provide third-party app stores as part of their activities. Other players develop app stores as their core activity, such as Steam, APKPure, Aptoide, F-Droid or GetJar. The business models, user base and number of apps available vary significantly from one third-party app store to another ([57]).

Most of these stores have various legal and technical means in place to avoid the risk that developers and users may use their services for illicit purposes. However, some experts explained that although some third-party app stores are following the standards of other stores and are compliant with regulations, others may be less pro-active than the bigger stores in enforcing such standards.

2.2.2 Apps sideloading

Just like other software, apps can be installed on devices through various means. Sideloading offers another way for users to download and install apps outside of any OS, device or third-party app store. Sideloaded apps ([58]) are made available in APK file format, through different means including dedicated 'APK sites' listing, providing details and explaining how to download and install such apps (including instruction videos). As with any other files, these APK files can also be shared through social media or messaging groups, or through shortened URLs pointing to locations where they are stored.

Some experts pointed to the fact that sideloading is also used on devices ([59]) supporting access to apps on television sets. In addition to users possibly sideloading IP-infringing apps on such devices,

([57]) A major third-party store such as Aptoide has over 430 million users and 1 million Apps. For more information, see the Aptoide website.
([58]) These are files that contains all the data needed for an app e.g. APK files for Android OS.
([59]) E.g. HDMI dongles or similar devices/boxes.

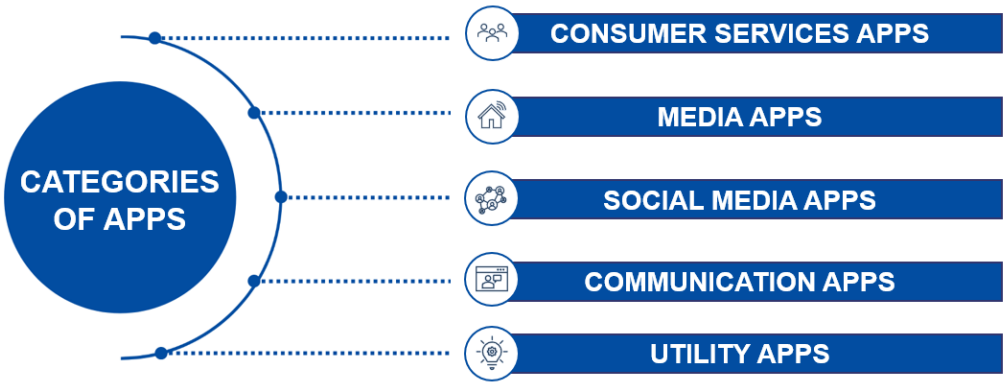
some IP infringers are also selling devices with pre-installed sideloaded apps, such as dual-purpose apps ([60]), in some cases bundling it together with illegal IPTV services.

In addition to IP-related risks, some experts also pointed to the potential higher risks ([61]) of users being exposed to harmful code such as malware with apps that have been sideloaded, as they may not go through the review processes typically put in place by operating systems, device manufacturers or some third-party apps stores. In that respect, some experts explained that, similar to anti-virus software, some apps can be used to scan all apps irrespective of the way they have been installed. When such apps find harmful content or code it triggers a warning asking the user if they still want to install it. Such apps are made available by some app stores ([62]) or by app developers ([63]).

2.3 Different types of apps, functionalities and business models

2.3.1 Main types of apps

Today, apps provide solutions for, inter alia, communication, entertainment, learning and productivity, and simplify a number of tasks for consumers and business users alike.



([60]) An example given by experts is the app 'Downloader'. This app is particularly popular with sports pirates as it helps to facilitate the download and installation of unauthorised live streaming apps onto streaming devices. Once the app has been installed, a user needs either a URL for the infringing app they are looking to install, or a numerical code that Downloader can create for the app.
([61]) It should be noted that apps that goes through a review process can also present a risk to its users, such as exposing them to malware or loss of personal credentials. See 'Fake LastPass password manager spotted on Apple's App Store', 2024, retrieved from BleepingComputer.
([62]) Google Play Protect. Last accessed on 28 March 2024.
([63]) 'Are Pirate Streaming Apps Dangerous? Using Free Tools is One Way to Find Out', 2023, retrieved from Torrent Freak.

There are different categories of apps used for various purposes, including the following.

- **Consumer services apps**: facilitate users' access to a broad range of existing services, such as banking, travelling, retail, transport and home delivery. E-commerce apps that allow third-party sellers to list products they sell on the app fall into this category.

- **Media apps**: facilitate access to content such as news, films, music, games, or user-created content, and can also be the app of a specific media (e.g. a newspaper, a radio station or a videogame) or aggregating different media or content (e.g. video sharing or music app). Media player apps that allow users to play content from different sources on their devices also fall into this category.

- **Social media apps**: support social connections by allowing 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 ([64]).

- **Communication apps**: support one-to-one communications (e.g. mail, instant message chat, call, video calls), as well as one-to-many and many-to-many (e.g. closed or open groups) communication. In many instances that kind of apps constitute private communication services ([65]).

- **Utility apps**: support a broad range of fairly basic services such as a calculator, to more advanced services such as productivity services (e.g. word processing), navigation and security (e.g. anti-virus and VPN).

([64]) See EUIPO's Social Media – Discussion paper on New and existing trends in using social media for IP infringement activities and good practices to address them, 2021. p.8.
([65]) See EUIPO's Social Media – Discussion paper on New and existing trends in using social media for IP infringement activities and good practices to address them, 2021. p.21 and 22.

2.3.2 Main apps functionalities

Although there are different categories of apps, only a few of their core functionalities are being used in the context of IP-infringing activities. These include the following.

- **Sharing of content**: with functionalities supporting upload, streaming or live streaming of content by the users. These functionalities can be used to illegally share IP-protected content, or to promote counterfeiting products (e.g. live streaming of video content presenting and marketing a counterfeit product).

- **Display of media**: with media player apps that can be created for perfectly legal purposes, but support access to IP-infringing files or streams. In that respect, experts pointed to specialised apps created for the sole purpose of sharing content illegally.

- **E-commerce**: with functionalities allowing brands to engage with customers, promote and market their products directly, or marketplaces allowing third-party sellers to do the same. With the rise of social commerce, a growing number of social media apps are integrating such functionalities ([66]). Some social media are also allowing their users to connect their e-commerce accounts within the social media app ([67]).

- **Communication**: with apps allowing private communications with other users or groups of users. Alongside their legitimate uses, experts pointed to the use of such apps ([68]) to engage with users in regard to IP-infringing products or services and to finalise transactions (e.g. private communication on ways to gain access and pay for the service). Closed group (i.e. invitation-only groups) are also typically used for IP-infringing activities to promote or sell counterfeit goods out of the public eye or to direct users to websites dedicated to such activities, or to exchange links to pirated content ([69]).

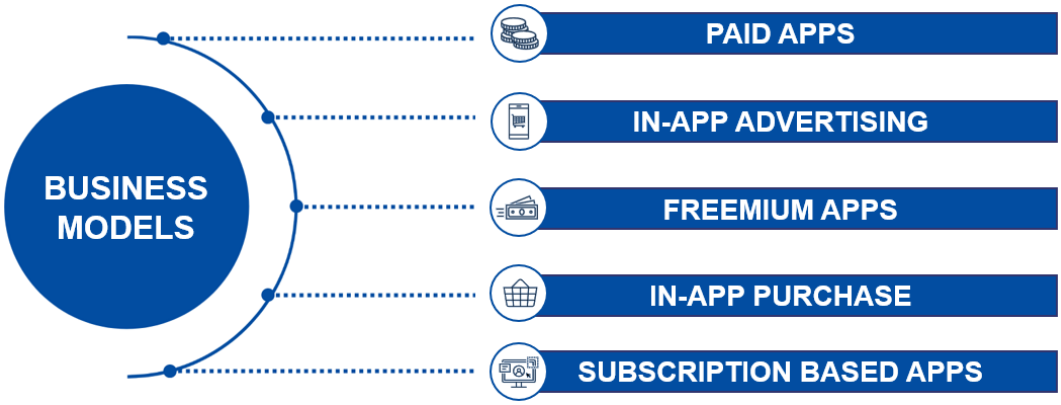
Some apps fall into multiple categories as they combine a set of functionalities. As explained in Section 2.1.1, this has led to the development of apps that are often referred to as super- or multi-

([66]) See, for example, TikTokShop.
([67]) 'Meta and Amazon team up on new in-app shopping feature on Facebook & Instagram', 2023, retrieved from TechCrunch.
([68]) E.g. Discord and Telegram.
([69]) See EUIPO's Social Media – Discussion paper on New and existing trends in using social media for IP infringement activities and good practices to address them, 2021. p.16.

purpose apps. Although these apps are very convenient for the user, they are also misused by bad actors, leveraging available functionalities to promote and market IP-infringing content and services.

2.3.3 Apps business models

Having in mind the fast-growing app economy, apps can be monetised through a variety of business models:



- **Paid apps** that need to be purchased. For example, utility apps such as smart calendars or media apps such as mobile games.

- **In-app advertising** with apps that can be downloaded for free but are displaying ads. This covers a broad set of ad formats including ads that are integrated into the app users' interface or form part of its content. In-app advertising can enable advertisers to target specific audiences and individuals based on their behaviour, preferences, device settings and location. It has grown quickly in recent years and is projected to reach around EUR 322 billion in 2024 ([70]). Just like other forms of online advertising, in-app advertising is misused by IP infringers to monetise their illegal activities.

- **Freemium apps** that are also offered for free but in most instances with basic functionalities or content. Revenues are generated by charging users who want to access more advanced functionalities or additional content. For example, a mobile game that only provides access to the first few levels, with the user having to pay to access further levels.

([70]) 'In-App Advertising – Worldwide', retrieved from Statista. Last accessed on 27 March 2024.

- **In-app purchases** that consist of selling physical or virtual goods through the app. For example, consumer goods brands can sell directly to their users through an app, or a mobile game can sell virtual items or extra games and bonuses to its players.

- **Subscription based apps** that require users to pay a regular fee to use them. For example, media or sports apps providing users with access to content. Some IP infringers are also misusing such models as a way to monetise their illegal activities.

These are the main business models, and app developers monetise their apps through a mix of them. IP infringers also leverage different business models and in particular in-app advertising and subscription-based apps to monetise their illegal activities([71]). In addition to legitimate business models, IP infringers may also engage in further illegal activities such as ad fraud or the dissemination of malware or the theft of personal data (see Section 3.2.1).

([71]) 'Advertising-funded digital piracy', 2023, retrieved from European Union Agency for Criminal Justice Cooperation (Eurojust).

3 Trends and challenges

This section explores the current IP-infringing trends in the field of apps and app stores and the challenges they raise for right holders, app stores and law enforcement authorities alike.

3.1 Trends in IP-infringing uses of apps and techniques to avoid enforcement

3.1.1 Pirated and fake apps

As explained in Section 2.1, the use and value of apps has evolved over time. It started with apps serving specific needs and having a value in themselves (e.g. utilities apps or mobile games) and developed to apps that are a new or complementary way for a number of businesses to provide their services and for brands to engage with their customers. This has led to the development of several IP-infringing trends.

- **App piracy** is a type of software piracy and consists of unauthorised copying, distribution and use of apps. The objective of the IP infringer is to deprive or divert paid downloads, ads or in-app purchase revenues from the original developers. For example, the pirated versions of apps can be slightly modified by IP infringers, to divert ad revenues by inserting ads from an ad network that pays them directly. These pirated apps are usually distributed through alternative app stores with no or limited control mechanisms in place. App piracy tends to be limited to certain types of apps, such as mobile games ([72]). This also includes **modified apps**, which are modified copies of original apps and provide users with access to new or improved functions, including unblocked premium functions, ad-free content, etc.

- **Fake apps** reproduce or imitate IP-protected names, logos and/or app interfaces of a company or brand with the aim of misleading users to believe that the app is genuinely from the company

([72]) 'The Mobile Economy Has A $17.5B Leak: App Piracy', 2018, retrieved from Forbes.

or brand. The objective of the IP infringer is in most instances to support other fraudulent activities. Fake apps can take different forms.

- **Apps for a trade mark that does not have its own app**. For example: in 2017 an app 'masquerading as MyEtherWallet.com, one of the internet's most popular services for storing ETH and other crypto coins' at the time made it to the top of the iOS App Store charts ([73]).

- **App cloning**, with IP infringers reverse engineering apps to access their source codes and add malicious code. In addition to copying the code of the app, IP infringers typically also reuse the app identifiers such as its name and package name ([74]). Despite the app looking the same, it performs or undertakes fraudulent activities. App cloning can affect all types of apps like social media ([75]), communication ([76]), media or utility apps ([77]).

- **App squatting**, with apps using confusingly similar version(s) of IP-protected names and/or logos of companies ([78]). App squatting is similar to the cybersquatting or typo squatting techniques used by IP infringers in the field of domain names ([79]), with the same objective of misleading users. Here again, the objective of IP infringers is to mislead users into installing apps used for fraudulent activities.

These types of apps can be distributed using different methods, including through app stores. They are used for a broad range of fraudulent activities that negatively impact the reputation of IP right holders, but also have harmful effects on users and advertisers.

([73]) 'Apple let a knockoff version of one of the world's biggest crypto wallets into the App Store', 2017, retrieved from TechCrunch.
([74]) The package name of an Android app uniquely identifies your app on the device.
([75]) 'Mobile Menace Monday: Facebook Lite infected with Spy FakePlay', 2017, retrieved from Malwarebytes Labs.
([76]) 'A review of cloned mobile malware applications for android devices'. Baykara, Muhammet & Colak, Eren. (2018).
([77]) 'Fake Netflix and thousands of popular apps injected with malware', 2021, retrieved from Pradeo.
([78]) 'Mobile App Squatting', Yangyu Hu, Haoyu Wang, Ren He, Li Li, Gareth Tyson, Ignacio Castro, Yao Guo, Lei Wu, and Guoai Xu. 2020. In Proceedings of TheWeb Conference 2020 (WWW'20), 20-24 April 2020, Taipei, Taiwan. ACM, New York, NY, USA, 12 pages.
([79]) See EUIPO's 'Domain Names Discussion Paper', 2021. p.7.

This may impact users as follows ([80]).

- **Billing fraud**, with apps automatically charging users in an intentionally deceptive way, including charging them to send a premium SMS or making a call to premium numbers without consent.

- **Denial of Service (DoS) attacks**, with apps participating in distributed DoS attacks without the users' knowledge, for example by sending a high volume of HTTP requests to produce an excessive load on remote servers.

- **Phishing**, with apps pretending to be from a trustworthy source to gather users' authentication credentials or billing information. Phishing may also be undertaken through in-app advertising placed on fake apps that, once clicked on, requires a user to complete a form or claim a 'fake prize'.

- **Spyware**, with apps transmitting personal data of the device and users without the user's notice and consent ([81]).

Advertisers can also be impacted in various ways, including the following.

- **Ad placement fraud**, with advertisers being misled into placing advertising on fake apps in the mistaken belief that these apps are legitimate or belong to a respected brand when instead they have been cloned or squatted.

- **Ad display and click fraud**, with apps deploying techniques to boost or fake user engagement or numbers often through the use of adware. These techniques mislead advertisers as to the numbers of ads viewed or engaged with, defrauding them into paying for views of the advertisement or traffic, when this was generated automatically and does not result from human activity. According to some experts, this mainly happens through piracy apps being designed with a code that executes clicks in the background without any visible ads to the

([80]) 'Malware Categories'. retrieved from Google Play Protect. Last accessed on 4 December 2023.
([81]) For example, see 'Fishing in the piracy stream: How the Dark Web of Entertainment is Exposing Consumers to Harm', Digital Citizens Alliance, April 2019, p.4 'As soon as a researcher downloaded the ad-supported illicit movie and live sports streaming app "Mobdro", malware within the app forwarded the researcher's Wi-Fi network name and password to a server that appeared to be in Indonesia.'

user, or activating a background app (e.g. launchers, memory cleaners, battery savers) at the same time as the user is on the piracy app in order to generate fake clicks. In addition, industry researchers have identified a similar technique, which they have termed 'Invisible Ads' ([82]), with apps loading advertisements while the device screen is off and generating advertising revenues. Again, such practices defraud advertisers paying for advertisements that are never viewed. It also negatively impacts users by draining battery life and unduly using mobile data.

- **Click injection**, with piracy apps monitoring the devices on which they are installed for signals sent from newly installed apps or apps whose status changed on that specific device. These 'install broadcasts' trigger the payment of commissions to the source of the app install (e.g. an online ad). In the case of click injection, the piracy app intercepts the 'install signal' and executes 'fake install clicks' even before the install of the app is complete. As a result, the piracy app operator receives credit and possibly commission for the fake installs.

3.1.2 Apps dedicated to IP infringing activities

3.1.2.1. Piracy apps

Piracy apps support illegal copying or distribution of copyright protected content such as music, movies, series or books. According to INTERPOL, '(i)nfringing apps have become the most prevalent emerging digital piracy method reported by police and private sector actors' ([83]). Experts pointed to **media players** playing a significant role in digital pirated content. Although some apps can be used to stream perfectly legal content, they are also somtimes used to illegally access content ([84]).

Once installed on a device, these player apps are fed with playlists ([85]) to view content illegally. These lists include a file that stores a series of URLs or IP addresses, which allow them to access broadcasts quickly and easily from various types of sources ([86]). These lists are made available by the providers of illegal services either directly to their subscribers or to users through websites, social media, or communication apps. Depending on the business models, these lists are made available

([82]) See 'Invisible Adware: Unveiling Ad Fraud Targeting Android Users', retrieved from McAfee. Last accessed on 23 January 2024.
([83]) See: Digital Piracy Methods, Project I-SOP, Online crimes targeting consumers governments and creative industries, INTERPOL, September 2023, p.2.
([84]) Experts have given examples of media players such as, IPTV Smarters; GSE Smart IPTV; Smart IPTV etc.
([85]) E.g. 'm3u playlists' (Moving Picture Experts Group (MPEG) version 3.0 Uniform Resource Locator).
([86]) Sports content, TV shows, films, music, etc.

for free or require payment. This can also influence the quality of the content and other connected services ([87]).

There are various types of piracy apps, both in terms of appearance and revenue model, in that respect ([88]) including the following.

- **Generic media players** that have a legitimate purpose but are being misused to access pirated content. These types of apps are usually offered for free and are financed through advertising placement or donations on the site. Due to their dual-purpose, experts have pointed to some specific challenges in relation to these apps (see Section 3.2.2). They point to some common characteristics of such apps, which gives away the piracy purpose of the app, including a built-in VPN to avoid geographical content access restrictions; user reviews highlighting the possibility of using the app to view paid or premium content for free; the provision of lists of Electronic Programming Guides ([89]) containing limited-use and/or paid channels; the use and supply of icons and logos of paid channels, sometimes integrated in the code of the app.

- **Custom branded media players** are media players branded with the name of the illicit IPTV service names. Although the app can typically be downloaded for free, a subscription is often needed to access pirated content.

- **Custom branded music apps** that are dedicated to illegal music consumption. Experts explained that these apps illegally share music from legal sources ([90]) to their users, with some apps built as search engines to retrieve music from different legal sources. These apps allow users to listen to music online, with some allowing users to download the music to the device itself, enabling the file to be copied to other devices. These apps are typically funded by ads but sometimes also have a subscription solution.

- **Streaming apps** that are offering access to illegal content such as movies and series. These apps are financed through monthly subscriptions and sometimes even advertising placement.

([87]) E.g. support services, access to passwords, regular updates.
([88]) 'A look at the problem, challenges and effects of App piracy', 2023, retrieved from Audiovisual Anti-Piracy Alliance (AAPA).
([89]) See Live Event Piracy – Discussion Paper: Challenges and good practices from online intermediaries to prevent the use of their services for live event piracy. EUIPO, 2023. p.35.
([90]) E.g. Spotify, YouTube and SoundCloud.

- **Live streaming apps** that are used for live content. Experts have pointed out that these types of apps are not that common due to their nature and that they usually have a name that clearly states the purpose of the app and hence will be removed by the app store. These apps are also generally offered for free, and the revenue stream stems from ads on the apps.

In addition to music and audio-visual content, **text content** can be found through apps illegally giving access to books, including academic textbooks and exam questions.

Some experts pointed to the fact that ads revenues paid to mobile publishers for the display of ads were much greater than those paid to website publishers, making apps particularly attractive and effective for IP infringers to monetise their illegal activities ([91]). In that regard, piracy apps financed through ads are sometimes unknowingly paid by legitimate brands through online ad campaigns ([92]). Some experts explained that due to the link with the rapid growth of ad spending on apps ([93]), and piracy apps building their audience through the exploitation of exclusive live content, and in particular live sport events, it was crucial to cut off ad revenues from piracy apps, referring to different initiatives in this field. (see Section 4.2.3.1).

3.1.2.2. Apps dedicated to the sale of counterfeit products

E-commerce has grown significantly in recent years, with business-to-consumer online sales increasing 82 % between 2016 and 2019 and a COVID-19-associated boost of 25.7 % in 2020 ([94]). This growth has slowed down in recent years due to people resuming more normal shopping behaviours. Mobile commerce with the convenience of apps to shop online have also contributed to this growth ([95]). Brands have seen apps as a way to connect more directly with their customers, building brand loyalty, gaining deeper consumer insights and reducing the need to rely on retailers and share the revenues with them.

([91]) See: Online advertising on IPR-Infringing Websites and Apps, EUIPO, February 2022, p.78.
([92]) 'Advertising-funded Digital Piracy', 2023, retrieved from European Union Agency for Criminal Justice Cooperation (Eurojust).
([93]) According to Statista, 'Ad spending in the In-App Advertising market was projected to reach US$314.50bn in 2023 and is expected to reach US$498.20bn by 2028'.
([94]) 'E-Commerce Challenges in Illicit Trade in Fakes: Governance Frameworks and Best Practices', 2021, retrieved from OECDiLibrary.
([95]) 'ECommerce App Development: Steps, Key Features, Trends', 2023, retrieved from uptech.

Some experts explained that in rare instances, apps are created for the sole purpose of selling counterfeited goods ([96]). Such apps are set up as standard e-commerce apps. Although some explicitly offer and advertise the counterfeiting nature of the goods for sale, some are more cautious, promoting products that are not evidently branded with third party brands.

Some apps promote themselves as **shopping agents** ([97]) rather than e-commerce providers. These apps are intended to help customers to buy from sites they can not buy from themselves, because, for example, the lack of shipping to that specific country or because the sites do not offer a domestic payment method. They offer services such as collecting and repacking, translation service of listings etc. These services could be perfectly legitimate, however, some providers actively help customers buying illicit products, such as counterfeits. The dual purposes of such apps complicates the detection and removal for the right holders in that it is not easy to clearly determine the actual purpose of the app, calling for further investigation such as test purchases etc.

3.1.3 Techniques used by IP infringers to evade detection and enforcement measures

3.1.3.1. Techniques to evade controls from app stores

As explained in Section 3.1, app stores have review processes in place to screen apps, as well as their updates, to identify illegal or harmful apps and activities, including IP infringement. The developers of these apps use a variety of techniques to try and defeat such controls, including:

- **piracy apps disguised as games** or another app seemingly having a legitimate purpose ([98]);

- **apps hiding malicious code from reviewers**, through encryption or delay with additional code being installed only after the initial installation or through updates ([99]) or non-disclosed new features or functionality;

([96]) Some experts referred to apps such as SaraMart and Voghion as examples they had identified at the time the discussion paper was drafted and may not exist anymore. Another example is an app called Vova. A court in the Netherlands found that the Vova platform had acted unlawfully by facilitating trade mark infringement. The court went on to say that the e-commerce platform must perform verification on their third-party sellers' actual identity using objective data and publicly disclose their identity. Furthermore, the court stated that the platform must take effective measures (including suspension of sellers) against re-occurrence of infringement on the same trade marks. See District Court The Hague 17 January 2024, ECLI:NL:RBDHA:2024:925.
([97]) 'Why the PandaBuy shopping agent should be on anti-counterfeiting radars', 2023, retrieved from World Trademark Review.
([98]) 'Devs Sneak Movie Piracy Apps Into App Store Disguised as Other Things', 2021, retrieved from TorrentFreak. See also 'Apple's App Store is Riddled With Popular Piracy Brands', 2024, retrieved from TorrentFreak.
([99]) See 'The 2023 McAfee Consumer Mobile Threat Report', p.6.

- **apps only behaving badly in certain countries/regions**: by checking the device location;

- **change app availability**, hiding the app from their account and subsequently on the app store during certain days of the week to avoid detection from right holders.

These different techniques are used by developers of fraudulent apps, which are sometimes referred to as 'maskware' ([100]), to benefit from the reach and trust of major app stores.

3.1.3.2. Techniques to get users to install IP-infringing apps outside of an app store

Experts pointed to the many techniques used by IP-infringing apps to get sideloaded by users, starting with making their apps available on the maximum number of APK sites to broaden their potential reach. They also pointed to promotion through social media posts, groups or specialised forums to share APK files directly or links to websites where it can be downloaded.

Experts also pointed to regularly deployed techniques, such as advertising on legitimate apps offering related content, or via social media ads and marketing. Once the users click on such ads they are directed to a website from where an APK file can be downloaded and providing detailed instructions on how to install it.

3.1.3.3. Techniques to escape or delay enforcement measures

According to some experts, a technique used by IP-infringing apps to avoid enforcement measures from app stores is to fake rights holder confirmation letters and/or letters of authority. Following a notification from a right holder pointing at the IP-infringing nature of an app or of its activities, the developer of the incriminated app sends such letters in an attempt to mislead the app store that they have a right to use the IP in question and try to escape or delay enforcement measures, putting the burden back onto the right holder to prove that the app does not have the right to use the relevant IP rights.

([100]) See Google Play Protect – Potentially Harmful Applications – Malware categories, last visited on 4 December 2023.

IP-infringing apps are also deploying different techniques to hamper or escape enforcement measures from right holders and law enforcement authorities, including the following.

- Piracy app with integrated Virtual Private Network (VPN) that is allowing users to hide their IP address and circumvent blocking measures or geolocation-based access restrictions to content ([101]).
- APK websites or APK files hosted on 'bullet-proof' hosting services 'that typically do not answer to notifications for illegal content, or legitimate requests for access to information about their users, and in many instances advertise their services as such. In some instances, it is not even possible to know where these services are operated from or to identify the legal entity in charge' ([102]).

3.2 Challenges

3.2.1 Identification of IP-infringing apps

Given the different type of apps that are being used for IP-infringing purposes, right holders and their representatives need to use different methods to monitor and review potential infringing apps. This poses different challenges for them and requires, sometimes, different software, hardware and knowledge.

3.2.1.1. Monitoring

As explained in Section 2.2, apps can be made available through different sources, which need to be monitored for IP-infringing apps.

- **Multiplication of app stores**: some experts pointed to the fact that although some app stores have review processes in place to prevent IP-infringing and fraudulent apps being made available on their services, the multiplication of third-party app stores was extending the range of app stores that needed to be closely monitored, particularly if they have limited or no review processes for apps that are being distributed through their app store.

([101]) See Discussion Paper on Live event piracy; Challenges and good practices from online intermediaries to prevent the use of their services for live event piracy, EUIPO March 2023, p.25.
([102]) Ibid. p.40.

In that respect, some experts referred to Article 6.4 Digital Markets Act ([103]) (DMA), which requires gatekeepers to 'allow and technically enable the installation and effective use of third-party software applications or software applications stores' ([104]). This provision aims to enable app developers to use alternative distribution channels and in addition allow end users to choose between different apps from different distribution channels. Therefore, it is expected that this provision will result in the introduction of alternative distribution channels for apps, including through alternative app stores.

In this context, it is worth noting that under the DMA ([105]), gatekeepers providing app stores are not prevented from taking measures, to the extent that they are strictly necessary and proportionate, to ensure that third-party apps and app stores do not endanger the integrity of the device or operating system, or that enable end users to effectively protect security in relation to third-party apps and app stores. In addition, the DMA applies without prejudice to the rules resulting from other EU rules applying to the provision of services covered by the DMA, such as the Copyright Directive and the Digital Services Act (DSA). As such, the DMA and DSA applications are complementary in ensuring that providers of alternative distribution channels, including third party app stores, will need to take responsibility for the content distributed through their services ([106]).

As part of the new regulatory framework provided by the DMA and DSA, some experts explained that a high level of protection in relation to apps used for fraudulent or IP-infringing activities, amongst others, may be one key element on which competing app stores would want to distinguish themselves from the gatekeepers. For instance, the DMA could enable providers of alternative app stores to compete with gatekeepers' security app review processes, ensuring higher levels of protection.

([103]) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).
([104]) On 5 September 2023, the European Commission designated Apple AppStore and Google Play, among others, as gatekeepers, retrieved from European Commission.
([105]) See Digital Markets Act, Article 6.4, subparagraphs 2 and 3.
([106]) In addition, although Article 6.12 of the DMA requires that gatekeepers apply fair, reasonable, and non-discriminatory general conditions of access for app developers to its app stores, it does not establish an access right and gives the ability for gatekeepers providing app stores to take the required responsibility in the fight against illegal and unwanted content as set out in the DSA.

Some experts also highlighted the development of new services facilitating the distribution of apps across a broad range of official and third-party app stores ([107]). They explained that this was adding to the need for them to extend their monitoring to multiple app stores.

- **Sideloading**: in addition to app stores, some experts explained that the multiplication of sources where apps could be sideloaded using APK sites was further extending the sources of potentially IP-infringing apps to be monitored. This also covered social media and forums where links to APK files are shared.

3.2.1.2. Detection

Some experts explained that the challenges in detecting IP-infringing apps vary significantly depending on the type of IP-infringing activities.

- **Apps piracy**: some experts explained that, as with illegal copy of existing apps, pirated apps were not particularly difficult to identify, and the challenge was really in crawling and monitoring the broad range of sources through which they could be downloaded.

- **Fake apps**: some experts explained that fake apps could be detected through monitoring tools used to 'crawl' app stores' data such as the names of apps and developers, metadata or images to identify the app using IP protected names, logos, or users' interface. They pointed to specific challenges raised by localised versions of apps and translation of metadata that required adaptation of keywords used by such tools. They also pointed to typo squatting, requiring advanced monitoring tools.

  Some experts explained that in some instances the IP infringement purpose was just to mislead users into downloading fraudulent apps that are obfuscating their malicious purposes to avoid detection (see Section 3.1.3). In this context, they considered that IP infringement in the name, metadata or logo of an app should be an indication of its fraudulent nature.

- **Apps dedicated to IP-infringing activities**: experts explained that information publicly available in app stores, or online in the case of sideloaded apps, may only provide an indication of the IP-infringing nature of the app. This could only be confirmed by downloading and using

([107]) See, for example, Catappult.io website and its App Distribution Console.

the app. They highlighted the specific challenges this raises in terms of investigative capacity to:

- set up accounts and monitor the content available through the apps, including subscribing to the IP-infringing app where this was the business model used;

- defeat some of the obfuscation techniques used by IP infringers, including geo restrictions of illegal content availability to certain countries or geographical areas.

3.2.2 Enforcement

Monitoring and detecting apps infringing IP rights are just the first steps, as the right holder or third-party enforcing its rights subsequently has to take action, which varies depending on the way the incriminated app is distributed.

- **Apps distributed through app stores**: although most app stores have procedures in place to notify IP-infringing apps ([108]), some experts explained that as a first step they were encouraging an amicable solution between the parties, which may delay the take down of apps even where there are blatant IP infringements ([109]). In addition, some experts explained that although most app stores have terms and conditions detailing the information a developer must provide to create a developer account ([110]) (see Section 4.1.2), IP infringers still manage to use misleading or fake contact details ([111]) to avoid legal actions. This in turn makes it difficult for the right holders to identify the developer behind an IP-infringing app.

  Experts have also pointed to the ease of uploading an identical app to several app stores at the same time, resulting in the need for them to file several notices for the same app. They explained that these stores have their own terms and conditions and requirements to file a complaint, and that depending on the regulations applying to the country where the app is offered, the store might just remove or restrict the download of the app in that country. The

([108]) Article 20 in the DSA will make this an obligation.
([109]) E.g. Apple dispute form and Google dispute form.
([110]) See also the new Digital Service Act and its rules about traceability of traders.
([111]) Experts have pointed to the importance of doing a thorough review of details submitted by developers. Here the new Article 30 of the DSA would help by collecting more reliable and complete information.

same applies to apps that are using third-party trade marks and design. These rights are normally territorial, and evidence must be submitted to prove rights in these specific countries.

With regard to piracy, some experts explained that some apps, purportedly disguised in a false appearance of legality, dissociate themselves from the illegal sharing of protected content they support, which is the core of their activities. These apps have terms and conditions highlighting their neutral nature with regard to the content used through their services, which do not reflect on the reality of the service provided. This may lead app stores to require additional information and proof of the illegal nature of the app from right holders before making a decision on whether to block or remove the app in question.

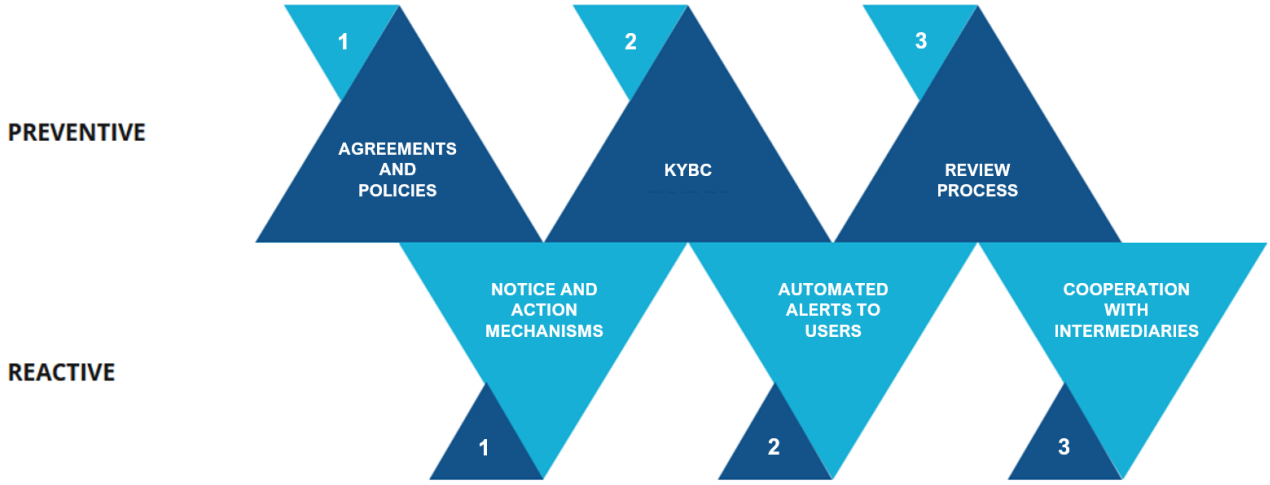
Some experts also pointed to the limits of the takedown processes from app stores, explaining that even if an app is taken down it stays on the devices where it has already been downloaded. Although updates and payments may no longer be processed through the app store ([112]), it continues to function. In that respect, some experts pointed to the fact that operating systems and devices related to app stores can disable the app from the device (see Section 4.2.1) or send warning messages to users of the apps removed from their app stores (see Section 4.2.2).

- **App sideloading**: some experts explained that sideloaded apps were raising the same challenges that arise in other types of piracy, with the need to notify hosting providers of APK files for IP-infringing apps. As with other forms of piracy, some of these hosting providers do not typically answer takedown requests, with some 'bullet proof' hosting providers advertising the fact that they were not responding to any takedown requests.

([112]) See for example Google Play policy on removed apps. Last accessed on 15 November 2023.

4 Good practices

Although apps and app stores are being misused in support of IP-infringing activities in several ways, a number of good practices to address such misuses have also been developed. This includes not only preventive and reactive measures ([113]) developed by app stores, but also cooperation with right holders and law enforcement authorities.



As explained in Section 1.3, while analysing such good practices, the Observatory and its experts worked on the understanding that some of the good practices identified in this discussion paper would be turned into regulatory obligations under the DSA and may also need to be adapted.

The implications of the Digital Services Act (DSA)

The DSA came into force on 16 November 2022 and is directly applicable across the EU to all regulated entities as of 17 February 2024 ([114]). As the new regulation setting up rules on the responsibilities of online intermediaries, its set of **cumulative obligations will apply to app stores** qualifying as the following.

- **Providers of intermediary services** with the obligation to include in their contractual **terms and conditions** information about the **restrictions** on the use of their service and

([113]) Preventive measures cover all measures implemented before an actual IP infringement occurs, and reactive measures cover the measures implemented in reaction to such an infringement.
([114]) Except for certain provision related to very large online platforms (VLOPs) and very large online search engines (VLOSEs) that are already applicable since 16 November 2022, as provided for by Article 93 of the DSA.

their **content moderation** policies, measures, tools and procedures, including algorithmic decision-making systems (Article 14).

- **Hosting services providers** with the obligation to put in place electronic and user-friendly **notice and action mechanisms** to remove or disable access to the **illegal content**, upon notification, in a timely, diligent, non-arbitrary and objective manner. The **individual or entity** that sent the notification **must be informed** of the decision taken based on the notification (Article 16). The decision must **also be communicated to any affected recipient of the service** (Article 17).

- **Online platforms** with the obligations to:
  - offer an **internal complaint-handling system,** open to both individuals and entities that have sent notices of presumed illegal content, as well as to any affected recipient of the service (Article 20);
  - give priority to notices submitted by '**trusted flaggers**' ([115]) (Article 22);
  - **suspend**, for a reasonable time and after a prior warning, the provision of services to users frequently uploading manifestly illegal content and set clear and detailed policies in their terms and conditions in that respect (Article 23).

- **Platforms allowing consumers to conclude distant contracts** with the following obligations to:
  - ensure the **traceability of traders** using their platforms by obtaining a certain amount of information, and before allowing them to use their services, make best efforts to assess whether this information is reliable and complete (Article 30). **For already existing traders**, the provider must make best efforts to obtain the information. If traders fail to submit the necessary information, the provider shall suspend the provision of the service to those traders.
  - make best efforts **to check whether the services offered on their platforms have been identified as illegal**, including randomly checking in any official, freely accessible and machine-readable online databases (Article 31).

([115]) Trusted flaggers are independent entities to be appointed on the basis of their expertise, for the purposes of detecting, identifying and notifying illegal online content.

- **Very large online platforms**' (**VLOPs**) ([116]). On 25 April 2023, the European Commission notably designated the Apple App Store and Google Play as VLOPs ([117]), with the obligations to:
  - diligently identify, analyse and assess any **systemic risks** related to their services, such as the **dissemination of illegal content** and the **negative effects on fundamental rights**, such as the right to (intellectual) property of right holders, taking into consideration their algorithmic and content moderation systems as well as terms and conditions (Article 34);
  - put in place reasonable, proportionate and effective **mitigation measures** addressing the identified **systemic risks**.

As a result, some of the good practices identified in this section are likely to be partly or fully turned into regulatory obligations ([118]).

4.1 Preventive Measures

A number of app stores and apps have measures in place to make sure that their services are not being misused for illegal or harmful purposes in the first place. This includes terms and conditions, guides, users' verification, as well as apps review processes.

4.1.1 App stores developer agreements and policies

The distribution and use of apps give rise to a chain of contractual relationships between:

- the **app developers and the app stores distributing their app**, which take the form of App Developer Agreements and App Store policies;

- the **app stores and the end users downloading the apps** through their services, which are typically referred to as Terms of Use or Service for users ([119]);

([116]) Under Article 33 DSA, VLOPs are the online platforms that meet the quantitative threshold of 45 million average monthly active users in the EU. The European Commission is tasked to designate VLOPs.
([117]) 'Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines', 2023, retrieved from European Commission.
([118]) This box is not meant to list all the obligations that applying to app stores under the DSA, but only the ones that are likely to result in identified good practices to be partly or fully turned into regulatory obligations.
([119]) See, for example, Apple, Google, Samsung and Amazon's terms of use. Last accessed on 15 November 2023.

- the **app developers and the end users using their apps**, which are also typically referred to as Terms of Use or Service.

This section only covers the app stores developer agreements and policies that can be used to undermine infringement of IP by the app itself (e.g. fake apps), and/or through its use of the app (e.g. piracy apps) ([120]). In most instances, the app developers' agreements set up general provisions on the need for the app and its use to respect IP, as well as on the consequences of not doing so, while policies provide further details and use cases.

As for **IP right infringement by the app itself**, developer agreements typically require developers to warrant that they have all IP rights related to their apps and that it does not infringe any third-party IP rights. Some app stores' policies further clarify that:

- this is not limited to the app itself but also extends to the metadata used to describe it (e.g. use of a protected trade mark as metadata) ([121]);

- apps that mislead users by using icons, descriptions or titles to impersonate another developer, company or entity are prohibited ([122]);

- apps that imply 'sponsorship or endorsement' or mischaracterises the relationship with a trade mark without permission of the relevant IP right holder are prohibited ([123]), with some policies going further in details in prohibiting the use without authorisation of names, logos or designs of sport leagues, clubs, players, movie, television and media celebrities ([124]).

Some experts pointed to such policies that include concrete examples of violations, as good practices to undermine fake apps that are supporting a broad range of fraudulent activities, which, in most instances primarily harm users (see Section 3.1.1).

([120]) The IP-infringing use of apps by end-users can also be address through the app's terms of use or service, as well as in-app reporting mechanisms and proactive measures from the app.
([121]) See, for example, Amazon Appstore Content Policy and Google Play policy center, Last accessed on 15 November 2023.
([122]) See, for example, Google Play policy center and Samsung Galaxy Store Distribution Guide Article 3.2. Last accessed on 27 November 2023.
([123]) See, for example, Amazon Appstore Content Policy. Last accessed on 15 November 2023.
([124]) See, for example, Samsung Galaxy Store Developers Intellectual Property Checklist. Last accessed on 27 November 2023.

As for **IP right infringement from the use of the app**, some app store policies are making it clear that:

- **apps that induce or encourage copyright infringement** are not allowed ([125]), with some policies going further in detailing prohibited activities, such as facilitating torrents, pirated software or illegal streaming and downloads ([126]);

- **apps that sell or promote the sale of counterfeit goods** are not allowed ([127]);

- **apps with user-generated content** and that can raise particular challenges including with regard to IP infringement, need to put in place a number of measures such as a method for filtering, reporting and blocking objectionable content and users ([128]);

- **apps supporting Artificial Intelligence (AI) generated content**: with app stores imposing on developers of such apps the requirement to have a reporting mechanism allowing users to report content that may be offensive or illegal, including IP-infringing content without exiting the app, as well as using reports from users to 'inform content filtering and moderation in their Apps' ([129]).

In addition, some app stores have contractual provisions in place to deal with apps and app developers that are not respecting their policies. In most instances, the app developers' agreements will set the contractual basis for the app store to take action ([130]), with the stores' policies providing further details on possible actions. In that respect some apps stores developer agreements or policies set up the following.

- **Actions that can be taken by the app store**, which in some instances include a broad range of possibilities. If the app infringes the app store's policies at the stage of the review process

([125]) See, for example Google Play policy center, Last accessed on 27 November 2023.
([126]) See, for example, Amazon Content Policy, Last accessed on 27 November 2023.
([127]) See, for example Google Play policy center, Last accessed on 27 November 2023.
([128]) See, for example, Apple App store review guidelines Section 1.2, Amazon Content Policy, Google Play policy center and Samsung Galaxy Store Distribution Guide Article 2.6. Last accessed on 27 November 2023.
([129]) See, for example, Google Play Policy Center on AI-Generated Content. Last accessed on 8 February 2024.
([130]) See, for example, Apple Developer Program License Agreement, Article 11.2, Aptoide Publisher Distribution Agreement, Article 10.1 and Google Play Developer Distribution Agreement, Article 8.3. Last accessed on 15 November 2023.

(see Section 4.1.2), it can simply be rejected. Where this happens after the review process, this includes the possibility of removing the app, suspending it until the violation is remedied, and limiting the visibility of the app in the store or its distribution in certain regions ([131]).

- **Repeat or serious violation policies**, making it clear that repeat infringement from a developer may result in the termination of this developer account ([132]). According to some experts this may lead to the deletion of that developer's apps from the store.

The analysis of different app stores' developer agreements and policies in the context of this discussion paper indicates that while major app stores tend to have specific and relatively detailed provisions to deal with IP infringement, this is not the case for 'smaller' stores. As for major app stores, the level of details of such provisions varies between the stores, and in some instances, they are spread across different agreements and information resources for developers.

Some experts highlighted the importance for app stores to effectively enforce their policies even at the app review stage (see Section 4.1.2), but also after they were made available on the app store, pointing to the lack of enforcement against IP-infringing apps by certain stores.

Some other experts explained that while clear cut decisions could be made on the IP-infringing nature of certain apps, it could be far more complicated in certain cases, and in particular with dual-purpose apps that could be used for both legitimate and IP-infringing purposes. In this context, they suggested that IP-infringing activities for such apps, may be better dealt with intermediary responsible for that specific app.

4.1.2 App stores Know Your Business Customer (KYBC) and user profile verification

App stores have several agreements and guidelines for app developers and typically require them to create a developer account. As part of the account creation, different requirements need to be met, including for the app store to identify and verify the legitimacy of businesses and individuals developing and publishing apps on their platforms. Although such KYBC requirements have been

([131]) See, for example, Google Play Enforcement Process.
([132]) See, for example, Amazon Appstore Content Policy, Aptoide Distribution Agreement, Article 10.4 and Google Play console help. Last accessed on 15 November 2023.

put in place by the app stores on their own initiative, the DSA now makes it an obligation with detailed criteria to meet to ensure the traceability of traders ([133]).

Major app stores have detailed instructions on the documentation and information developers need to provide to create an account and subsequently upload apps to the store, whilst other stores have less detailed instructions and require less information ([134]).

Most stores differentiate between individual and business developer accounts.

- **Individual account**: the developer typically needs to provide basic information like legal name, postal and email addresses, and phone number. To comply with the requirements of the DSA, some stores also require the developer to submit a copy of their ID ([135]).

- **Business account**: the developer needs to provide a legal name of the company, postal and email addresses, phone number and if applicable, the company's website address ([136]). In addition, specific business identifiers, for example a D-U-N-S number ([137]), may be required, as well as proof that the person creating an account has a legal right to do so ([138]).

Some app stores verify different types of information using different methods including:

- one-time verification code being sent to the number and/or email provided ([139]);
- checks on information provided including from third-party providers and various sanctions databases, mainly in relation to ID verification ([140]);

([133]) See the Digital Service Act, Article 30.
([134]) See for example Aptoide 'Catappult Certified Developer Distribution Agreement'. Last accessed on 8 February 2024. Instead of asking for detailed information when an account is created, some stores only require the developer to accept the developer agreement, which includes, inter alia, paragraphs where the developer guaranties they are a legal business and that they are authorised to represent that business, hence putting the onus on the developer.
([135]) See Apple's 'Enrolling, verifying, and renewing with the Apple Developer app' and Google's 'Required information to create a Play Console developer account'. Last accessed on 8 February 2024.
([136]) If a website address has been provided, it will need to go through a verification process and checks are carried out to make sure that the website is connected to the developer. See for example Apple's 'Enrolling, verifying, and renewing with the Apple Developer app' and Google's 'Verify your developer identity information'. Last accessed on 8 February 2024.
([137]) See dun & bradstreet website. Last accessed on 8 February 2024.
([138]) See, for example, footnote 2 in Apple's 'Enrolling, verifying, and renewing with the Apple Developer app'. Last accessed on 8 February 2024.
([139]) See for example Google 'Verify your developer identity information' and Amazon 'Create a developer account' Last accessed on 8 February 2024.
([140]) See for example footnote 2 in Apples 'Enrolling, verifying, and renewing with the Apple Developer app'. Last accessed on 8 February 2024.

- specific device and/or software access requirements ([141]);
- verification of financial information, including through the processing of the developer membership payment, which can help verify the identity of the developer and through various sanctions databases ([142]).

4.1.3 Review process

Once a developer has created an account, major app stores review the apps submitted before making them available. This process comprises reviews of the app's business model, technical performance including permissions required, design, content and privacy implications ([143]). Some app stores are also implementing specific checks for apps installed from alternative app stores or directly from the web ([144]). These review processes are intended to identify harmful and illegal apps, including IP-infringing apps.

The process is similar across major app stores performing reviews and starts when developers upload their apps and associated metadata (e.g. title, description, developer name, screen shots, size, version) to their developer accounts. Major app stores review or at least prohibit similar types of information and functionalities, including the following.

- **Content review** focusing on content that can cause harm to the user's health, encourage illegal behaviour or excessive consumption of harmful products, or have other objectionable content, particularly if the app targets children. In addition, as explained in Section 4.1.1, if the app supports the sharing of user generated content, some stores ([145]) check that the app has certain functionalities in place, such as the ability to moderate and report content, block abusive users and easily contact the developer.

- **Performance review** focusing on the app's functioning as per the description provided by the developer. This includes a review of the app's metadata to ensure that it correctly reflects the

([141]) See for example Apples 'Enrolling, verifying, and renewing with the Apple Developer app' and Google 'Verify your developer identity information'. Last accessed on 8 February 2024.
([142]) See Google 'Verify bank account'. Last accessed on 8 February 2024.
([143]) See for example, Apple's App store review process, Google Play review process and Amazon App Store review process. Last accessed on 15 February 2024.
([144]) See for example Apple's Notarization for iOS apps in the EU. Last accessed on 15 February 2024.
([145]) Some smaller stores do not seem to have specific rules about apps containing user generated content. See for example Catapult (Aptoids distribution platform) Submission Process. Last accessed on 16 February 2024.

app's core functionalities experience. As part of the app description, the developer is not allowed to promote content or services that it does not offer. The functioning of the app should be clear to the user, and it should not include any hidden or dormant features or functionalities. In addition, the app should be self-contained in that it is not allowed to download, install, or execute outside code that introduces or changes features and/or the functionality of the app, or of other apps ([146]).

The performance review also consists of verifying the permissions required by the app and of security checks for malware and viruses, including for functionalities that may alter or disable native user interface elements or behaviour. Some app stores also require the personal account developer to have their apps tested by a closed group of users for a period of time before it can be published on the store ([147]).

- **Payment and business models review** focusing on the apps payment and subscription models. Although the app stores do not dictate what developers should charge for their app and connected services, they check the information provided about the price and business model to ensure it is clear for the user and not deceptive. If the app is financed through ads, these will need to comply with the stores' policies and not act in a fraudulent manner such as render ads that are not visible to the user or send fake installation attribution clicks to get paid for installations that did not occur ([148]).

- **Legal review** focusing on the compliance of the app with relevant legal requirements. This may include review of the app's privacy policy and how that data is managed. The app should also not collect data or request access to device functionalities that are not relevant to its core functionality. Developers that submit apps related to specifically regulated activities, such as banking, must prove that they are authorised for such activities. As part of the review process, app stores can also request developers to prove that they own or have rights on the IP rights contained and/or shared within the app, but also in its metadata and code.

([146]) See for example, Apples App store review process. Last accessed on 16 February 2024.
([147]) Google require their developers to test the app on a group of 20 testers for a duration of 14 days before it can be published. See Googles App testing requirements for new personal developer accounts. Last accessed on 16 February 2024.
([148]) See Google Ad Fraud policy. Last accessed on 16 February 2024.

The review process can be repeated numerous times if there are changes or updates made by the developer before, during and after the app's publication ([149]).

4.2 Reactive Measures

App stores have also put in place some measures to handle and act upon IP related complaints from users and right holders. These include notice and action mechanisms, as well as alert systems for when an app has been deleted from a store.

4.2.1 Notice and action mechanisms

The notice and action mechanisms ([150]) allow any user and interested party such as IP rights holders, to notify app stores of apps or app content that may be in breach of relevant laws or app stores' policies, for it to take action ([151]).

To simplify and streamline the notification process, some app stores have implemented guided notification processes via web forms. Pre-filled forms and guided steps facilitates the submission of notices for different types of IP infringement through apps ([152]), including:

- use of a trade mark to cause confusion, and/or preventing a trade mark owner from using it as an app name, which can be used to notify fake apps, including app squatting (see Section 3.2.1);
- copyright infringement with apps unlawfully using copyright protected works, which can be used to notify piracy apps (see Section 3.2.2.1);
- counterfeit, which can be used to notify apps dedicated to the sale of counterfeit products (see Section 3.2.2.2);
- apps that are used as tools to bypass technological measures protecting copyrighted works.

([149]) Retrieved from Apple Developer Program License Agreement, section 6.
([150]) As explained at p. 38, having a notice and action mechanism in place is now a regulatory obligation for hosting providers under Article 16 of the Digital Services Act.
([151]) See, for example, Flag an app or review on Google Play and Report a Problem on Apple Store. Last accessed on 15 November 2023.
([152]) See for example, Google Play and Apple App Store. Last accessed on 15 November 2023.

App stores typically require specific information from right owners reporting an IP infringement, including, as a minimum, the reporter's name, email address and country of legal residence, as well as information on where the disputed app can be found in the app store (normally through a URL), as well as the type and clear description of the IP infringement ([153]).

Some app stores require information about existing IP rights (e.g. trade mark certificates and copies of copyrighted work and where authorised work can be found), evidence that the complainant is the owner of those rights or authorised to file the complaint and, if applicable, where these rights are registered ([154]). Stores that do not require a submission of evidence will verify the rights holder by the information submitted in the form ([155]). Some stores also allow for a reporter to submit one notice for several apps that are infringing an IP right.

Once they have received a notice, some app stores will evaluate and decide on whether to take down the app, suspend its distribution, or keep it available. Other app stores encourage the right holders and the developer of the reported app to resolve the issue ([156]) amongst themselves before the store takes any action.

Where an app is removed or suspended it remains functional on the user's device. However, it can not be updated, and no payments to the app developer are processed. Initially, neither a warning, a suspension or a rejection of an app will have an impact on the developer's account. However, if the app is removed from the store it could lead to the developer account termination, especially if this is a re-occurring event. Some stores allow developers to re-submit their app under the condition that they make the necessary changes to the app, so they comply with the policies ([157]).

Some experts pointed to this limit of the apps removal from app stores, highlighting the possibilities for operating systems and devices related to app stores to actually disable the app from the device. They explained that if this was limited to fraudulent activities other than IP infringement, there were

([153]) See for example Apple App Store Content Dispute, Report Content On Google, Samsung Intellectual property (copyright, trademark) infringement report (requires login) and Aptoide Terms of Service Section 10. Last accessed on 16 February 2024.
([154]) See for example Report Content On Google and Samsung Intellectual property (copyright, trademark) infringement report (requires login). Last accessed on 16 February 2024.
([155]) See for example Apple App Store Content Dispute. Last accessed on 16 February 2024.
([156]) See for example Apple App Store Content Dispute. Last accessed on 16 February 2024.
([157]) See for example Google Play information on removed apps. Last accessed on 16 February 2024.

reported discussions to apply such disabling to IP-infringing apps ([158]), as well as a first judicial injunction in Spain ordering three app stores to disable users' access to a piracy app ([159]).

4.2.2 Automated alerts to users

Some app stores send out warnings to users about potentially harmful apps they are about to install from their stores, or that they have installed on the same device from other sources (e.g. sideloaded apps). These notifications are generated automatically, informing the user of the reason for the notification based on a pre-determined list of potential harm, including different types of frauds, malwares, spam or phishing activities that may affect the users or their devices ([160]). In some instances such systems may block the app or recommend or require for it to be run through security checks ([161]).

Some experts explained that such systems performed similar functions to anti-virus software installed on devices running apps. Although they are not directly related to IP-infringing activities, they undermine the installation and use of IP-infringing apps supporting fraudulent activities harming users and advertisers (see Section 3.1.1). In this regard, some experts suggested that specific alerts could also be sent to the users of apps removed from apps stores due to IP infringement, as a way of informing users.

4.2.3 Cooperation initiatives

4.2.3.1. Cooperation from the advertising sector

As explained, with in-app advertising growing fast and projected to reach around EUR 322 billion globally in 2024 (see Section 2.3.3), IP infringers are monetising their illegal activities, defrauding advertisers with fake or pirated apps used for ad placement, display or click frauds (see Section 3.1.1) or monetising their audience with piracy apps displaying ads (see Section 3.1.2.1).

([158]) 'LaLiga "Talks to Google" About Deleting Piracy Apps From a Million Phones', 2023, retrieved from TorrentFreak.
([159]) Magistrate Court No. 1 of Cieza of 27 April 2022.
([160]) See Google Play Protec Warning Strings for Malware and Unwanted Software. Last accessed on 11 November 2023.
([161]) See Google Play Protect Developer Guidance for Google Play Protect Warnings. Last accessed on 11 November 2023.

In addition to providing a revenue stream to IPR infringers, the presence of advertising for legitimate brands on websites and mobile apps that infringe IPR can confuse consumers. It can lead them to mistakenly believe that the site or app they are accessing provides access to legal content, goods or services' ([162]). In that respect, a number of good practices are developing to cut off monetisation of piracy apps through branded advertising, including the following.

- **Memorandum of understanding on online advertising and IPR** ([163]): as part of its 'follow the money' strategy, the European Commission 'invited companies and associations from the advertising industry and other interested stakeholders and technology providers to sign a MoU on online advertising and IPR (…)' ([164]). The MoU was signed in 2018, with signatories representing parties involved in placing, buying, selling and/or facilitating advertising, including advertisers, advertising agencies, trading desks, advertising platforms, advertising networks, advertising exchanges for publishers, sales houses, publishers, and IPR owners. The signatories committed themselves to minimising the placement of advertising on IPR-infringing websites and mobile apps to deprive them of the revenue flows that make their activities profitable.

  The MoU has proven effective with regard to ads displayed on websites, with the first report on the functioning of the MoU published in 2020 showing a 12 % decrease in the average number of ads collected per visit to IPR-infringing websites monitored following the introduction of the MoU ([165]). As for apps, the first analysis that would serve as a basis for future monitoring was published in 2022. It estimated that the annual revenue generated worldwide by the 543 monitored apps was EUR 57.1 million for 2021 ([166]).

- The **Trustworthy Accountability Group** (TAG) launched the TAG Pirate Mobile App Tool to help members prevent their advertising from appearing on apps that are known for distributing pirated content ([167]). TAG's Anti-Piracy Working Group also developed and launched the Piracy

([162]) See: Online advertising on IPR-Infringing Websites and Apps, EUIPO, February 2022, p.7.
([163]) See European Commission website on Memorandum of Understanding on online advertising and IPR.
([164]) See Report on the functioning of the Memorandum of Understanding on online advertising and intellectual property rights, August 2020 p.3.
([165]) Ibid, p.10.
([166]) See: Online advertising on IPR-Infringing Websites and Apps, EUIPO, February 2022, p.10.
([167]) The Anti-Piracy Working Group at TAG has created a collection of best practice recommendations to assist advertisers, agencies, and mobile ad tech intermediates in identifying and removing infringing mobile applications from their advertising inventory. The framework for businesses to utilise and contribute to the TAG Pirate Mobile App Tool, which helps them find and stop mobile apps that violate their rights, is another one of these recommendations. Retrieved from TAG's website.

Mobile Apps List (PMAL), a shared list to help members identify fraudulent apps and avoid displaying their ads on them ([168]). Some experts pointed to such tools as reliable sources listing piracy apps, as well as existing commercial services offering verification of apps before their onboarding by media buying agencies and advertisers. Such services were mentioned as tools available to advertisers in running checks and identifying potential risks and exposure for their brands to be associated with piracy services, and their ads to finance such services.

In addition to good practices from advertisers to prevent their ads from appearing on IP-infringing apps, some experts pointed to the fact that AdTech companies serving ads through the integration of their SDK (see Section 2.1.2) in an app, should also check apps using their SDK against the existing IP-infringing apps list.

4.2.3.2. Cooperation with Law Enforcement Authorities

In addition to the set of good practices that can contribute to take down or demonetise IP-infringing apps, some experts pointed to the need for cooperation with Law Enforcement Authorities to investigate and dismantle the criminal groups behind these kinds of activities. Some experts highlighted good practices with law enforcement operation at the EU and international level, targeting piracy apps, including the following.

- **Specific operations supported by EUROPOL**, and, for example, its cooperation with the Spanish National Police following a complaint from a number of sports rights holders about a mobile app illegally offering live content through a number of platforms located in Spain and Portugal and connections to servers in the Czech Republic. This operation led to the take down of the app that was used by more than 100 million users ([169]). Some experts explained that this operation was illustrating the scope and cross border nature of live event piracy operations, as well as the risk of such activities, because on top of financing its activities through advertising, the Spanish company behind these illegal activities was also selling its user information to a company related to botnet and DDoS attacks.

([168]) According to TAG, the PMAL is released on a quarterly basis and provides information 'needed to stem the flow of ad revenue to mobile Apps with pirated content'. Retrieved from TAG's Report 'WINNING THE FIGHT AGAINST AD-SUPPORTED PIRACY'.
([169]) See 'Illegal mobile application with more than 100 million users taken down in Spain', Europol, March 2021.

- **Operation 404**: a multi-jurisdictional effort led by Brazil that started in 2019 to fight against digital piracy in Brazil and other Portuguese-speaking countries. The *Operation 404* entered its 6th phase, focusing on digital piracy on illegal streaming, music and games websites and apps. As part of the 5th phase, the Brazilian authorities cooperated with authorities in Peru (Indecopi) and the United Kingdom, (UKIPO and PIPCU). In addition to arrests, this phase of the operation led to the blocking of 199 illegal streaming sites and 63 apps that were used to broadcast audiovisual content such as series, games and music, in the three countries. It also led to the blocking of six messaging app channels that were used to illegally distribute music.

In relation to law enforcement activities, some experts pointed to the European Commission IP Action Plan from 2020, which called for the capacity of law enforcement authorities (…) to be substantially strengthened, and for counterfeiting and piracy to become a higher priority ([170]). They also pointed to the European Commission Media Action Plan from 2020, which invited EU policy makers to explore how existing remedies to fight against piracy, such as injunctions, can be made more efficient and easier to obtain, notably in order to cope with the dynamic and borderless nature of online commercial-scale infringements ([171]).

5 Conclusion

The increased use of apps and app stores have brought about many benefits for consumers and businesses. It has also attracted illegal and fraudulent actors misusing apps in the context of their activities, including IP-infringing activities. Experts have identified several trends in that respect, that do not only harm right holders, but also users exposed to cybersecurity threats, or advertisers falling victims of new ads fraud techniques. Experts also brought to light specific techniques used by infringers to avoid or delay enforcement actions from app stores and right holders, highlighting the specific challenges to enforce IP rights in the app ecosystem.

This paper was drafted at a time when the major regulatory changes brought about by the DSA were coming into play. As a result, some of the good practices identified in this paper will be turned into regulatory obligations or may have to be adapted to comply with the DSA. Beyond new regulatory requirements, the good practices identified would hopefully contribute to further the understanding

([170]) Communication from the European Commission, 'Making the most of the EU's innovative potential An intellectual property action plan to support the EU's recovery and resilience', 2020, p.15.
([171]) Communication on 'Europe's Media in the Digital Decade: An Action Plan to Support Recovery and Transformation', 2020. P.21.

on different practices that are implemented to undermine the misuse of apps and app stores in the context of IP infringing activities.

Considering the increasing importance of apps, as well as regulatory, technical and market developments driving the development of good practices, the EUIPO will keep monitoring and documenting the development of good practices to effectively address IP infringement through apps.