

Advisory Committee on Enforcement

Seventeenth Session
Geneva, February 4 to 6, 2025

CHALLENGES AND GOOD PRACTICES TO PREVENT THE USE OF APPS AND APP STORES FOR IP INFRINGEMENT ACTIVITIES

*Contribution prepared by Mr. Antoine Aubert, IP Digital Specialist, European Observatory on Infringements of Intellectual Property Rights (EUIPO Observatory), European Union Intellectual Property Office (EUIPO), Alicante, Spain**

ABSTRACT

Apps are now a major channel for users to access content and a diversity of services ranging from e-commerce to banking. The use of apps has also moved beyond mobile devices to all connected devices such as smart TVs and smart watches.

Apps are typically distributed through app stores, particularly Google Play and Apple's App Store. Some device manufacturers and other third parties have developed their own app stores. Apps can also be downloaded and installed outside of an app store.

While the increased use of apps and app stores brings benefits for consumers and businesses, it has also led to their misuse for illegal and fraudulent activities including IP-infringing activities.

This contribution is based on a EUIPO Observatory discussion paper that analyzes the misuse of apps and app stores for IP-infringing activities, the challenges this raises, and most

* The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO.

importantly good practices to address such misuses¹. It will help different stakeholders to better understand how to address the issue.

I. EVOLUTION OF THE APPS LANDSCAPE

1. Over the past 15 years, there has been a notable increase in the number and usage of apps. In 2023, consumer spending on app stores reached 171 billion United States dollars, with users spending over five hours daily on apps. That same year, 257 billion new apps were downloaded, averaging 489,000 downloads per minute².

2. While apps have become a major means for users to access a wide range of content and services, including e-commerce and banking, they are also an important element of brand strategies to engage with consumers. Apps have expanded beyond mobile devices to other connected devices, including smart TVs that support app downloads from manufacturers or third-party stores. Television sets can run apps via gaming consoles and HDMI dongles, or similar devices that can be plugged in. In recent years, super-apps have emerged, offering a range of services like e-commerce, monetary transfers, delivery, transport, communication and social networking under one platform. While these super-apps are mainly popular in Asia, 'light' versions are developing in Europe.

3. Apps are typically pre-installed on connected devices or downloaded from an app store. Just like other software, apps can also be downloaded and installed from outside an app store (known as sideloading). Sideloaded apps are made available in the Android Package Kit (APK) file format through different means, including dedicated websites that list such apps and provide details on how to download and install them. APK files can also be shared through social media, messaging groups and shortened URLs.

II. MISUSE OF APPS AND APP STORES FOR IP-INFRINGING ACTIVITIES

4. While the increased use of apps and app stores is beneficial to consumers and businesses, it has also led to their misuse for illegal and fraudulent activities, including different types of IP-infringing activities. Such activities include the following:

- a. Infringement of IP rights on legitimate apps. Just like other software, apps can be illegally copied in part or in full. With pirated copies of legitimate apps often distributed outside of the main app stores that are often used to spread malware or adware, or IP-protected parts of successful apps (such as code, user interface and functionalities) that are illegally copied or replicated. In some instances, IP infringers build on components of successful apps to design apps that are then used to spread malware or adware.
- b. Infringement of third-party IP rights through apps with app squatting consisting of using the protected name and/or visuals of a company to confuse users into believing the app is from this company. Like cybersquatting, this can mislead users and drive traffic to apps that are fraudulent, spread malware, infringe on IP rights, provide access to pirated content or sell counterfeit products, or to dual purpose apps that have a perfectly legitimate use but are mainly or exclusively used for IP-infringing purposes.

¹ European Union and Intellectual Property Office, *APPS & APP STORES - Challenges and good practices to prevent the use of apps and app stores for IP infringement activities*, available at: <https://www.euipo.europa.eu/en/publications/apps-app-stores-challenges-and-good-practices>.

² data.ai, *State of Mobile 2024 – The Industry's Leading Report*, available at: <https://sensortower.com/state-of-mobile-2024>.

c. Misuse of legitimate apps by IP infringers as part of their illegal activities with apps supporting marketing and payment for IP-infringing goods and services, such as social media or payment apps and private communication and messaging apps that are misused as part of IP-infringing activities to provide information, support, or finalize transactions.

5. Some of these IP-infringing activities do not only harm right holders but in some instances are also used to defraud users, with spyware spread through piracy apps or apps impersonating a legitimate brand, that transmit personal data of the device and users without the user's notice and consent. They can also harm advertisers that suffer from ad placement fraud, thinking they are placing ads on legitimate apps when they are fake or cloned.

III. TECHNIQUES USED BY IP INFRINGERS AND ENFORCEMENT CHALLENGES

6. IP infringers are deploying different techniques to evade detection from app stores, right holders and subsequent enforcement mechanisms. This includes apps disguised as games, or other seemingly legitimate apps to hide their illegal purposes. Malicious apps can also disguise harmful code to escape detection through app store review by using encryption or activation delay. Some piracy apps have also integrated virtual private networks (VPNs) to hide users' IP addresses and circumvent blocks or geolocation restrictions.

7. Counteracting the misuse of apps and app stores for IP-infringing activities raise specific monitoring, detection and enforcement challenges. While some app stores have review processes to prevent IP-infringing and fraudulent apps from being listed, the increase of third-party app stores requires closer monitoring of stores with limited or no review processes. In addition to app stores, the increase in ways apps can be sideloaded further expands the sources of potentially IP-infringing apps that must be monitored. This includes monitoring of social media and forums where links to APK files are shared.

8. As for the detection of IP-infringing apps, different methods must be used depending on the functionality of the app and its source. IP right holders may need to use specific hardware and software to install and inspect the app to determine its IP-infringing nature.

9. Regarding the enforcement against IP-infringing apps available in app stores, even if such apps are removed from the store they remain on the users' devices and can continue to be used. Like any other form of piracy, IP-infringing apps that are sideloaded raise challenges, with the need to notify the hosting providers of the APK files. As with other forms of piracy, some of these providers do not typically answer takedown requests, with some hosting services advertising the fact that they are not responding to any takedown requests at all.

IV. GOOD PRACTICES TO COUNTERACT THE MISUSE OF APPS FOR IP-INFRINGING ACTIVITIES

10. Some app stores, right holders and law enforcement authorities have implemented practices to prevent the misuse of apps for IP-infringing activities. This contribution is based on a discussion paper that was drafted before February 2024 and the full application of the Digital Services Act (DSA), with the understanding that in the European Union some of the good practices identified would become regulatory obligations or may need to be adjusted to comply with this new regulation.

11. The DSA is setting up rules on the responsibilities of online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms and app stores. The new rules include, but are not limited to, an obligation to have clear and easily accessible terms and

conditions, provide transparency reports, implement notice and action mechanisms and implement a trusted flagger scheme. All online intermediaries offering their services in the European Union, whether they are established inside or outside the European Union, must comply with the new rules. The European Commission will enforce the DSA together with national authorities who will supervise the compliance of the platforms established in their territory.

PREVENTIVE MEASURES

12. Several app stores and apps implement measures to prevent the misuse of their services for illegal or harmful purposes. In app stores, developer agreements and policies are setting up general provisions regarding the requirements an app needs to fulfil, including on IP-related matters.

13. As for IP right infringement by the app itself, developer agreements typically require developers to ensure that they have all IP rights required, and that the app does not infringe any third-party IP rights. Some app stores' policies are going further in clarifying that this is not limited to the app itself but also extends to the metadata used to describe it (such as the use of a protected trademark in the app metadata), or that apps misleading users by using icons, descriptions or titles to impersonate another company or entity, or that are mischaracterizing the relationship with a trademark owner without permission are prohibited.

14. As for IP right infringement that may arise from the use of the app, some app stores are prohibiting apps inducing or encouraging copyright infringement or require apps with user-generated content to put in place measures for filtering, reporting and blocking objectionable content and users. Regarding generative Artificial Intelligence (AI) apps, some app stores require them to have a mechanism in place for users to report content that may be offensive or illegal, including IP-infringing content, as well as using such reports to 'inform content filtering and moderation' in their apps.

15. Some app store policies also detail the sanctions developers can face if they do not comply, such as removal and/or suspension of the app and, in some cases, termination of their developer account.

16. As part of the creation of an app developer account, app stores typically require different information to identify and verify the legitimacy of businesses and individuals publishing apps on their platforms. Although such requirements have been put in place by some app stores on their own initiative, the DSA now makes it an obligation in the European Union with detailed criteria to be met to ensure the traceability of traders³.

17. Once a developer has created an account, major app stores review the apps submitted before making them available. This process comprises reviewing the app's business model, technical performance (including permissions required), design, content and privacy implications. Some app stores are also implementing specific checks for apps installed from alternative app stores or directly from the web. These review processes are intended to identify harmful and illegal apps, including IP-infringing apps, and can be repeated numerous times if changes or updates are made by the developer before, during and after the app's publication.

³ See Article 30 of the Digital Services Act, available at: https://www.eu-digital-services-act.com/Digital_Services_Act_Article_30.html.

REACTIVE MEASURES

18. Some app stores have also put in place measures to handle and act upon IP-related complaints from users and right holders. This includes notice and action mechanisms, allowing 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. Some app stores have implemented guided notification processes via web forms to simplify and streamline the process. Pre-filled forms and guided steps facilitate the submission of notices for different types of IP infringement.

19. Some app stores also send warnings to users about potentially harmful apps they are about to install, or that they have installed on the same device from other sources (for example, sideloaded apps). These notifications are generated automatically, informing the user of the reason for the notification based on a pre-determined list, including different types of fraud, malware, spam and phishing activities that may affect the users or their devices. Such systems function similarly to anti-virus software. While they are not directly related to IP-infringing activities, they prevent the installation and use of IP-infringing applications that engage in fraudulent activities affecting users and advertisers.

20. With in-app advertising growing fast and projected to reach around 322 billion euros globally in 2024⁴, some IP infringers are monetizing their illegal activities by defrauding advertisers with fake or pirated apps used for ad placement, display or click frauds. Some are also monetizing their audience with piracy apps that display ads. In addition to providing revenue stream to IP infringers, the presence of advertising for legitimate brands on IP-infringing apps can lead consumers to mistakenly believe that such apps provide access to legal content, goods or services⁵.

21. In this respect, some good practices aim at cutting off monetization of piracy apps through branded advertising. This is the case for the European Commission Memorandum of understanding (MoU) on online advertising and IPR⁶ that was signed in 2018 by parties involved in placing, buying, selling and/or facilitating advertising. Within the MoU, parties commit to minimizing the placement of advertising on IPR-infringing websites and mobile apps, in order to deprive them of the revenue flows that make their activities profitable. Similarly, the Trustworthy Accountability Group (TAG) also launched the TAG Pirate Mobile App Tool to help its members prevent their advertising from appearing on apps that are known for distributing pirated content⁷.

V. CONCLUSION

22. The increased use of apps and app stores has many benefits for consumers and businesses, and just like websites in the past, they have become an important element for brands to engage with users. However, just like most new digital developments, apps and app stores are also misused for illegal and fraudulent activities, including IP-infringing activities. This includes several trends that do not only harm right holders, but that also harm users, who

⁴ Statista, "In-App Advertising – Worldwide", available at: <https://www.statista.com/outlook/amo/advertising/in-app-advertising/worldwide>.

⁵ See: European Union and Intellectual Property Office, *Online advertising on IPR-Infringing Websites and Apps*, p.7, available at: <https://www.euipo.europa.eu/en/publications/online-advertising-on-ipr-infringing-websites-and-apps>.

⁶ See: https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/memorandum-understanding-online-advertising-and-ipr_en.

⁷ The Anti-Piracy Working Group at TAG has created a collection of best practice recommendations to assist advertisers, agencies and mobile ad tech intermediaries in identifying and removing IP infringing mobile apps from their advertising inventory.

are left exposed to cybersecurity threats, and advertisers that fall victim to new ad fraud techniques.

23. Beyond new regulatory requirements in the European Union, the good practices identified in this contribution aim to help with their general application, and further the understanding on measures that can undermine the misuse of apps and app stores in the context of IP-infringing activities.

[End of document]