A LOOK AT THE PROBLEM, CHALLENGES, AND EFFECTS OF APP PIRACY

According to Verimatrix, there are around 7 billion mobile devices in use as of 2023, all of which are connected to the internet and use multiple Apps. Statistics from data.ai (formerly App Annie) show that, in 2021, two million new Apps were launched, and 230 billion Apps were downloaded. That’s >435,000 App downloads per minute! Given those figures, there’s no doubt that Apps are an integral part of our daily routine, so much so that 3.8 trillion hours were spent using them in 2021. That’s 4.8 hours per day or, put another way - a third of our waking hours, and roughly an hour per day more than people in the U.S. spend watching broadcast TV. How does that data translate into revenue?

App spend just from iOS, Google Play, and Third-Party Android in China reached USD170 billion in 2021, equating to >USD320,000 per minute, and mobile ad spend reached USD 295 billion. Moreover, our appetite for Apps shows no signs of slowing down. Statista reports that global mobile App revenues will hit USD613 billion by 2025. With online Pirates
renowned for adapting and following popular trends, it’s no surprise they want a piece of the mobile App action. But what is App piracy, what are the challenges and its effects, and are we doing enough to stop it?

**What is App Piracy?**

Before we jump in, let’s break down App piracy. Digital piracy is a broad term. It covers the access, use, or distribution/streaming of protected content without the rights holder’s permission, whether that is unlawful copies of copyrighted movies, TV programs, e-books, games, music, or software. What does AAPA define as App piracy? It is the unauthorised modification and/or distribution of Apps by someone other than the official rights owner.

**Why are Apps appealing to pirates?**

Besides the popularity of Apps, there are four key reasons why smart applications have become the go-to distribution method for Pirates.

1. The ease of set-up provided by off-the-shelf development kits.
2. The ability to host Pirate Apps on official App stores.
3. A reduced level of investment is required, and the vetting process (or what the Digital Services Act refers to as “Know Your Business Customer”) is almost non-existent in most App stores.
4. Smart TVs, STBs, Dongles, and mobile devices use Android as an Operating System.

Why do Pirates prefer Android? With Android controlling the mobile OS market with close to 72% share, compared to iOS, accounting for around 28%, they can reach a wider audience. Unlike closed, proprietary iOS, Android publishes an Android Package Kit (APK). Why does this matter? Pirates can obtain APKs and change the code within them for illicit reasons, resulting in new users downloading a modified APK instead of the original App. But let’s be clear. App piracy is not just an Android or Google Play problem. It’s a global issue across all the App stores.

**What’s the difference between the various unauthorised Apps?**

Pirates exploit our love of Apps in several ways, but first, let’s start with the different types of unauthorised Apps. There’s a difference and it’s essential to grasp as it has a bearing on what’s expected of the rights holder to demonstrate that their App and associated content has been pirated.

Illicit Apps are those that a Pirate has stolen directly or illegally duplicated, without permission. Typically, they will remove attribution – the identification of the rights holder, for instance, logo. Pirates redirect or replace advertising and disable tracking functionality before republishing the Apps on one or many App stores, including their Pirate monetisation solutions.

There are content-agnostic Apps that can play legal and unauthorised content. It’s up to the user to choose what content they consume.
In the battle of online piracy, the burden of proof lies with the rights holder, meaning that for the content-agnostic Apps, there is an additional hurdle to overcome. The rights holder must prove who is behind the content-agnostic App, demonstrate that it is being used to share their content without authorisation, and show how the App is being promoted.

Why does the promotion of the App matter? As the TorrentFreak article explains, how the Apps are promoted plays a part in determining their legality. For instance, if a developer promotes their App for infringing purposes, the link to it being deemed illegal becomes stronger – even if there’s an absence of infringing content on the App itself. Based on what we have seen to date, these illicit Apps are typically only promoted by Pirates.

**What are the different types of Pirate Apps?**

To understand the problem, let’s dig deeper into the different types of Pirate Apps used and highlight how Pirates generate revenue. At AAPA, we categorise illicit Apps into four categories.

- “IPTV” generic media players
- Custom-branded IPTV
- Live streaming sports
- Movies and series streaming

**“IPTV” generic media players** are Apps created for illicit functions. However, the media players are not, in their own right, illegal. The players can be content-agnostic Apps or Apps developed for Pirates. But as explained earlier, there is – more often than not – an illicit connection to such “IPTV” generic media players.

**Custom-branded IPTV** are typically white-labelled Apps developed by Pirates or Apps branded using the illicit IPTV service name.

**Live streaming sports** are Apps used for unauthorised content. Generally, these are white-labelled Apps developed by Pirates. As only a few developers produce these Apps, it’s common to see a generic templated approach in their look, feel, and functionality.

**Movies & series streaming**, similar to the category above, are Pirate-developed Apps used for unauthorised content.

When it comes to how Pirates generate revenue, we regularly see Pirates charging subscription or monthly fees for custom-branded IPTV Apps and those Apps streaming movies & series.

Exploiting the user’s personal data is another revenue angle. As INTERPOL explains, some Piracy services may sell user data, such as browsing history or personal information, to third-party companies. Distributing malware is another avenue some Pirates utilise to line their pockets.

But far and away, Ad words campaigns are the most lucrative for Pirates. Yes, not only are rights holders losing money from the lack of legitimate App downloads, but Pirates steal what should be their ad revenue as well.
**How much is piracy costing the industry?**

Pirates make a lot of money. Don’t be fooled by the many piracy Apps claiming to offer “free” content.

Quite honestly, it is naïve to think Pirates do it as a goodwill gesture. They are not charities, handing out access to content to ease the economic pressures. Quite the opposite. Pirates are in it for the money. They are often large, international organisations spread across different jurisdictions, with IT infrastructure and sizeable resources. Like legitimate organisations, Pirates need revenue to stay in business. The difference is that Pirates get their income at the expense of the rights holders. How much money are we talking about?

The Digital Citizens Alliance, August 2021, paper, *Breaking (B)ads: How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market* reported that through advertising and subscriptions, the operators of piracy platforms are estimated to generate a combined USD2.34 billion dollars in annual revenue.

Looking specifically at the ad revenue of Pirate digital media worldwide between June 2020 to May 2021, Statista reported that it generated an estimated USD1.34 billion. Approximately 20% of the total came from in-App advertising. With global mobile App revenues rising, the Pirate share will also grow.

**What’s the impact on users?**

Not only are Pirates impacting the financial health of the audio-visual industry at large, but they also pose a danger to regular users.

The main risks to piracy users include having their bank details stolen or their personal data leaked (e.g. user/passwords, credentials, and contacts). They can fall victim to Adware campaigns, leading users to download and install other Apps by clicking on the ads. And, of course, there is a risk of malware. A 2022 study for AAPA on malware and audiovisual piracy found that if you use an App to access pirated content, you have a 57% chance of it coming with embedded malware.

Beyond the main risks, a piracy user could also fall prey to being locked out of their device or having their data deleted. The user’s credentials could even be used in carrier billing fraud. There is also a risk of location tracking, eavesdropping, or stenography.

**What are the challenges with Pirate Apps?**

We can break down the challenges into three categories: App stores, processes, and devices.

**App stores**

The fact that Pirate Apps are available to download from official App stores adds an air of legitimacy. Most trusting users believe downloading from an official App store means the Apps and the developing organisation have been vetted and are legal.
Process
As with streaming piracy, there is a complex and/or lengthy process for submitting takedown notices. All the while, users can still download the Pirate App. When a takedown notice is finally issued, App owners or developers can appeal the takedown, which keeps the App available in the store for even longer.

Devices
Even if the rights owners successfully have the Pirate removed from the App store, downloaded Apps remain on the users’ devices. The user still has access to pirated content.

What can be done to stop App piracy?
Content owners and broadcasters already undertake disruption activities to erode the viewing experience on Pirate sites and Apps, encouraging viewers to seek premium quality, legitimate alternatives. There is also the hope that users will leave a poor rating about the Pirate App, causing others to think twice before downloading it.

For App piracy, many challenges content owners and broadcasters face could be minimised by closer cooperation with the App store owners. Collaboration is the key to reducing the threat App piracy presents to the audio-video industry. What would this look like in practice?

Preventing new Pirate Apps from being available on App stores
Making it harder to access Pirate Apps will likely deter most average App users, leaving only the truly determined to hunt down where to find them. How can we go about this?

Preventing new Pirate Apps from appearing in App stores can be split into two activity streams.

From an App store perspective, implementing a robust process around the Digital Services Act “Know Your Business Customer” could eliminate a lot of Pirate organisations slipping through. For instance, requesting a copy of identification, legal evidence of its rights to stream the content, or even the App store validating the App before publishing.

Optimise the removal of branded Pirate Apps
A study of over a million Apps on Google Play Store in 2019 found approximately 50,000 potentially counterfeit or infringing Android applications. Admittedly, Google Play is the largest, but that’s just one of the many App stores. What can we do?
Working together to introduce faster, streamlined processes to remove Pirate Apps on the App stores could dramatically cut down the number of downloads.

These processes could make it easier for Trusted Flaggers to report Apps that infringe content and establish an approach to prevent Pirate App owners and developers from submitting counterclaims to take down notices and agreeing on a repeat infringer policy. Another way for App stores to remove Pirate Apps could be to leverage automatic detection, using defined keywords, such as Free IPTV or Free football, to highlight the illegal Apps quickly.

But for a long-term solution, like all forms of digital piracy, we are stronger when we act together. Beating the online Pirates requires all parties across the audio-visual ecosystem to collaborate and work together if we ever hope to beat this very present and pervasive threat.

Pedro Bravo
Head of Content Protection
NOS