Handbook on Intellectual Property in Mobile Applications

2024

TABLE OF CONTENTS

Figures

Tables

Key

This work uses text boxes to bring to the reader certain additional information, such as sector statistics, examples, mini case studies and checklists, in an easy-to-read manner. These text boxes are color coded, with the following colors:

Orange	Statistics, examples
Green	Tips
Yellow	More information
Purple	Case Studies
Grey	Checklists and Key Takeaways

Chapter 1. Current status and trends

1.1. Introduction

The proliferation of smartphones and digital technology has been astronomical – witness the number of mobile apps being used worldwide. These apps, ranging from gaming, entertainment and social media platforms to banking and health, have become an integral part of our daily lives, transforming how we interact, communicate and access information. According to the online statistics portal Statista, in 2022, mobile app engagement increased only 3 per cent year-over-year, while between 2019 and 2022, the time spent using mobile apps rose by approximately 46 per cent, with users globally spending more than five and a half hours daily using apps.

While mobile social media and communication platforms still rank as the most engaging app category, they decreased slightly in 2023, down to 42.4 per cent of all global time spent among smartphone users, from 43 per cent in 2021. The box below provides some further statistics in the mobile app sector for 2023:

Key mobile app statistics for 2023

- Mobile apps generated around 500 billion United States dollars in revenue in 2023.
- Apple App Store has 1.96 million apps available for download.
- There are 2.87 million apps available for download on Google Play Store.
- 21 per cent of Millennials open an app 50-plus times per day.
- 49 per cent of people open an app 11-plus times each day.
- 70 per cent of all digital media time in the United States of America comes from mobile apps.
- The average smartphone owner uses 10 apps per day and 30 apps each month.

Source: TechReport and Statista

Not only are mobile apps an essential part of our lives, they also have an important impact on the economy, especially in developing and fast-growing countries. For

example, India's app economy (including sales of apps, in-app purchases, subscriptions, advertisements, public relations) is expected to hit 792 billion United States dollars by 2030, contributing 12 per cent to the estimated GDP.[1]

As the statistics demonstrate, mobile apps have an important role, and all the more so in the near future. For this reason, it is crucial to understand the app ecosystem, economy and legal protection, which is the purpose of this handbook.

In this introductory chapter, the dynamic realm of mobile applications will be outlined, and the most recent trends and developments analyzed. We will begin by identifying and scrutinizing the sectors that are currently at the forefront of mobile apps. Second, the trending technologies in the context of apps will be examined, and finally, the types of applications that are gaining momentum in the mobile app ecosystem will be categorized and analyzed.

This introduction serves as a critical roadmap, allowing readers to navigate the upcoming chapters with greater clarity. In the subsequent chapter, we will delve into topics such as the mobile apps ecosystem, IP protection for mobile apps, IP contracts and financing strategies. By providing this contextual foundation, our aim is to empower readers through a comprehensive understanding of the multifaceted world of mobile applications, facilitating a more in-depth exploration of the topics that lie ahead.

1.2. Preview of the sector

1.2.1. Structure

The mobile app sector exhibits a multifaceted market composition, encompassing a spectrum of key parties ranging from well-known, established technological leaders to autonomous developers and nascent entrepreneurial ventures. This inherent diversity contributes to innovation and the uninterrupted introduction of novel apps. Nevertheless,

[1] Jain, R., *et al*. *The Economic Value of the App Economy in India*. Broadband India Forum, June 2023. <www.broadbandindiaforum.in/wp-content/uploads/2023/06/Research-paper-on-THE-ECONOMIC-VALUE-OF-THE-APP-ECONOMY-IN-INDIA.pdf>.

it is important to understand that the structural configuration of the sector displays the dominance exerted by major application distribution platforms – app stores – notably exemplified by Apple's App Store and Google Play Store, and even the Huawei AppGAllery, particularly in China.

1.2.2. Market concentration

The level of market concentration within the mobile app sector undergoes variations at distinct stages of its life cycle. During the conception and development stages, a higher degree of fragmentation prevails. This period witnesses a dispersion of entities such as independent developers, development agencies and other stakeholders as ideas for apps originate from universities, start-ups, small and medium-sized businesses, artists and other creatives, and established businesses. As to platforms (defined as operating systems for app devices), a significant concentration arises around Android and IOS.

In the distribution stage, a notable concentration also emerges. Prominent app stores such as Apple's App Store and Google Play exert significant influence in terms of both app downloads and revenue generation. This has triggered apprehension concerning their practices, prompting anti-trust complaints and regulatory scrutiny, such as the EU Digital Markets Act, aimed at ensuring equitable competition and averting anti-competitive conduct.

As for the associated technological services such as mobile app hosting, payment gateways and mobile payment and advertising services, the fragmentation is repeated. This environment allows a multitude of entities to participate, fostering a diverse market landscape.

Finally, with mobile operators, the degree of market concentration and dominance (or not) of significant actors tends to differ according to a country's development. In some countries with lesser developed markets for mobile operators (and sometimes a national or private monopoly), these operators get more involved in the app market, and may, for example, charge percentages on transactions. In more developed markets, greater

competition between mobile operators and broadband providers ensures that apart from their own mobile app offerings, which may be significant, their intervention is principally limited to being data carriers.

1.2.3. Investment

Investment in this sector has surged in recent years, especially between 2020 and 2021, with peaks related to the COVID-19 pandemic, which made anything mobile an attractive target for investors. High potential returns due to diverse monetization strategies, such as in-app purchases and advertisements (see chapter 3), has attracted significant interest from investors. Venture capital firms actively supported start-ups, and other diverse opportunities. Despite a decrease in investment from 2021 to 2022, the trend continues to evolve and grow, making it an attractive choice for investors seeking innovation and profitability.

1.2.4. Policy attention

Policymakers have acknowledged the significance of overseeing the mobile app industry to promote fair competition, safeguard consumers and ensure personal data are protected, among other objectives. Efforts such as the European Union's Digital Markets Act (DMA) and Digital Services Act (DSA), and the General Data Protection Regulation (GDPR), aim to tackle issues linked to the dominance of app marketplaces and higher risks in terms of privacy within Europe. This is not limited to the European Union. Regulations including the Personal Data Protection Act in Singapore, the Australian Privacy Principles and India's Digital Personal Data Protection (DPDP) Act, 2023 share the common goal of establishing clear guidelines and responsibilities, mainly for app stores, but also for the whole mobile app sector, while upholding the rights of end users.

1.3. Trending sectors

From how we shop and communicate, to the ways we learn and relax, there is an app for virtually every facet of human existence and sector of the economy. As with any evolving landscape, certain sectors within the app environment have experienced

exponential growth. The following sectors have been particularly prominent in recent years, and we provide examples and statistics in boxes.

Food delivery and grocery. With the rise of the on-demand economy, food delivery and grocery apps have experienced unprecedented growth, especially after the COVID-19 lockdowns. Convenience and accessibility have become paramount, with users enjoying the ability to order meals and groceries with a few taps on their smartphones.

Food delivery and grocery statistics

The numbers are astonishing. In 2023, the user base of online food delivery apps and platforms reached 3 billion consumers, while for 2024, grocery delivery has a projected market value of 1.22 trillion US dollars.

Outstanding apps in these sectors include: (1) Uber Eats, the most widely available, with activities in the six continents, (2) DoorDash, leader in the United States of America, and (3) Delivery Hero group brands, such as talabat in the Middle East and PedidosYa in Latin America.

Source: Statista

Gaming. Gaming apps have transformed the entertainment industry, with a dedicated and expanding user base. From casual games such as Candy Crush to immersive multiplayer experiences, mobile gaming continues to captivate audiences worldwide.

Gaming numbers

As of 2023, almost 700,000 games were available in mobile app stores. Revenue in the mobile games market was projected to reach 173.60 billion US dollars in 2023. Most of this was expected to be generated in the United States of America. In 2022, the top genres, by gross revenue, were role play, strategy and puzzle.

Source: Statista

Entertainment. Entertainment apps have become integral to everyone's daily lives, regardless of age. Streaming platforms such as Netflix, Disney+ and Spotify have redefined how people consume content and media, offering a vast library of content at our fingertips. Personalized recommendations and on-demand access make entertainment apps a staple for those seeking quality content.

Entertainment statistics for 2022

In 2022, the leading entertainment and streaming app worldwide by number of downloads was TikTok, with more than 670 million downloads, followed by Netflix, with 165 million downloads, YouTube, with 154 million, and Disney+, Amazon Prime Video, YouTube Kids and HBO Max

Source. Statista

Mobile learning. Education, especially after the COVID-19 pandemic, has gone mobile, with learning apps catering to learners of all ages. These apps offer courses, tutorials and resources on a wide range of subjects, empowering users to expand their knowledge and skills anytime, anywhere. Mobile learning is particularly valuable in a world where lifelong learning is essential for personal and professional growth.

Mobile learning apps

Mobile learning is the second largest category in Google Play, and the third largest in Apple Store, with Duolingo the top education app, with 49 million users

Source: Business of Apps

E-commerce. Shopping apps have transformed the way we shop, providing a convenient and secure platform for online purchases. E-commerce giants like Amazon and Alibaba have paved the way for smaller retailers and entrepreneurs to reach global audiences, fostering a competitive and dynamic marketplace.

Ecommerce apps sales

Analysts expect 3.5 trillion US dollars of mobile e-commerce sales by 2027.

Source: Statista

Banking and payments. Mobile banking and payment apps have become indispensable for managing finances and making transactions. They offer features such as mobile check deposit, budgeting tools and peer-to-peer payment options, simplifying financial tasks and promoting cashless transactions.

Banking and payments apps

An estimated 2.8 billion mobile wallets are in use worldwide, almost half of them in Asia-Pacific. Numbers are increasing in Canada, United States of America and Europe, though South-East Asia lags far behind.

Source. Tranglo

Well-being and fitness. The health and well-being sector has seen a surge in mobile apps, catering to fitness enthusiasts, mental health advocates and those seeking healthier lifestyles. These apps offer features such as workout tracking, meditation guidance and nutrition planning, empowering users to take control of their health.

Well-being and fitness examples

The more popular apps in this sector are Strava, MyFitnessPal and the meditation app, Calm. Revenue in this market sector was projected to reach 85.5 billion US dollars for 2024, with an expected annual growth rate of 12.4 per cent for 2024.

Source: Statista

Cryptocurrency apps. The rise of cryptocurrencies has spawned a new wave of apps for buying, selling and managing digital assets. These offer real-time market data, wallet services and secure trading platforms, catering to novice and experienced crypto enthusiasts.

Cryptocurrency apps

The Cryptocurrency app market had a revenue of 541.34 million US dollars in 2022, and an estimated value of USD 639.16 million in 2023, with Binance and Coinbase as the largest operators.

Source: FinTechFutures.

Overall income per sector. The following figure 1.1 illustrates the sector and amount of revenue generated worldwide in the mobile app industry:

Figure 1.1 Worldwide mobile app revenue

Source: Armstrong, M. “Games dominate global app revenue.” statista.com. Feb. 27, 2023. <www.statista.com/chart/29389/global-app-revenue-by-segment/>.

1.4. Trending technologies

In the last couple of years some technologies have been widely used in mobile applications. The following, in particular, have improved user experience or app functionality and are particularly relevant for intellectual property (IP) protection and management:

Artificial intelligence: AI and machine learning (ML) have become integral to app development. AI-powered algorithms analyze user data to provide personalized experiences, recommend content and optimize user interfaces. ML models enhance app functionality by enabling predictive analytics, automating tasks and improving user engagement. From virtual personal assistants to chatbots, AI and ML are shaping the future of app interactions.

Examples of apps using Artificial Intelligence

- Spotify, the music streaming app, uses AI to create personalized playlists for users.
- Grammarly, the online writing assistant and grammar checker tool and app, uses AI to correct grammar and spelling.
- FaceApp, which modifies photos and videos, uses AI to edit photos to make users look older or younger.

Augmented reality and virtual reality: AR and VR are revolutionizing the way users interact with apps and the real world. AR overlays digital information on to the physical world, while VR immerses users in entirely digital environments. From gaming and education to health care and retail, these technologies offer limitless possibilities for creating engaging and immersive experiences.

Examples of apps using Augmented or Virtual Reality

- Google Lens uses AR to overlay information about topics in the real world. For instance, it can be used to identify plants and landmarks.
- The IKEA app uses AR to enable users to see how furniture would look in their home.
- Pokemon Go uses AR to enable users to find Pokemons in the real world and catch them.
- Job Simulator app uses VR to enable users to experience different jobs and work, for example, as mechanics, surgeons and in other roles.

Peer-to-peer: P2P technologies took off in the early 2000s but are now becoming popular in the app sector as they enable user-to-user communication. Without the need for intermediaries, these apps allow for file sharing, communications and even money transactions. P2P apps, which provide efficiency and convenience, are revolutionizing how people connect and conduct business.

Examples of apps using P2P technologies

- WhatsApp, the instant messaging app, uses P2P technology to send messages between users.
- Send Anywhere, an app for easy file sharing, uses P2P technology to transfer files between devices.

- PayPal, the online payment platform and app, uses P2P technology to allow users to send and receive money.

Security technologies: as the app ecosystem grows, so do security threats. App developers are prioritizing security by implementing robust encryption, biometric authentication and application programming interface (API) security best practices. Continuous monitoring and updates are essential to safeguard user data and maintain trust.

Examples of apps using high security technologies

- WhatsApp, the instant messaging app, and others like Telegram, use end-to-end encryption to protect all messages.
- Payment apps, such as PayPal or Venmo, secure their APIs to connect users with bank servers using the security protocol HTTPS and other measures.

5G: 5G technologies allow real-time experiences, from high-quality video streaming to augmented reality applications, due to its speed and low latency. Serves as the foundation for Internet of things (IoT), connected devices, live streaming and real-time gaming applications.

Examples of 5G apps

- Netflix offers 5G connection in some countries to allow users to stream content in ultra-high definition (HD).
- Call of Duty Mobile uses 5G technology to provide a better experience for users, with a more realistic and immersive gaming experience.

Voice technology: revolutionizes how we use apps. Voice-activated assistants, including Siri and Alexa, have gained widespread recognition. To increase accessibility and user engagement, app creators are using voice recognition and synthesis.

Voice Technologies

- Several virtual assistant apps, including Siri, Amazon Alexa and Yandex Alice, use voice technology as a core technology.

Near-field communication: contactless transactions and data sharing are becoming simple due to NFC technology, which is easing daily activities and providing convenience and security for anything from mobile payments to using public transport.

NFC apps

- NFC is widely used by mobile payment apps to allow contactless payments and payments with smartphones, communicating payment information between the user's phone and merchant's terminal.
- Apps using the technology are Google Pay, Apple Pay, Visa PayWave and Venmo.

Natural language processing: empowers apps to understand and respond to human language. Chatbots and virtual assistants use NLP to engage users in natural conversations, making information retrieval and customer support more efficient.

Natural language processing apps

Grammarly uses NLP to identify grammar, spelling and punctuation errors in text.

Many virtual assistant apps use NLP to understand and respond to user requests, including DuerOS, Yandex Alice and Xiaoice.

In terms of IP, while most, if not all, of these app-related technologies are implemented mainly in software code and, therefore, primarily protected by copyright, they are also the subject of an increasing number of patent applications worldwide, particularly in China, Europe and the United States of America. Patents are important for hardware-related technologies such as NFC, voice technologies, communications and embedded security. They are also closely and increasingly related to the datasets generated by apps (for training and fine-tuning AI models, for example) that may have regulatory (for

personal data) or contractual protection as well as becoming significant trade secrets, as will be discussed in Chapter 4.

1.5. Trending types of mobile applications

After outlining the trending sectors in the app environment, and the latest technologies they use, it is useful to define apps that are becoming more popular and frequent.

Super apps: a prominent trend in the mobile app ecosystem is the rise of super apps, multi-purpose applications that offer an array of services and functionalities within a single platform. They aim to be a one-stop solution for users, eliminating the need to download multiple specialized apps. In technology terms, super apps are particularly sophisticated and complex, with a greater need for understanding and managing IP-related issues.

Super apps

The global super apps market size was valued at 61.30 billion US dollars in 2022, and is expected to expand at a compound annual growth rate (CAGR) of 27.8 per cent from 2023 to 2030. Examples of super apps include WeChat, Gojek, Rappi and Alipay.

WeChat began as a popular messaging app in China in 2011 but has evolved to a comprehensive platform. It counts 1.3 billion monthly active users, and is the most famous super app in the world.

It offers everything from voice calls and video calls, to file sharing, payments, gaming and transportation, and also integrates with other services such as Alipay and Baidu Maps. A versatile app, it meets the needs of many Chinese users.

Source: Statista / Grand View

Native apps: apps that are specifically developed for a particular operating system using platform-specific programming languages (such as Swift for iOS, or Java for Android). Native apps are optimized for the respective platform, resulting in a superior user experience and performance. Further, they have a seamless integration with the device's

hardware and software features that means better performance and functionality. Popular native apps include Instagram, WhatsApp, Spotify, Uber and Netflix, for iOS and Android, showcasing how tailored experiences contribute to popularity. Such tight integration with the app platform may mean negotiating specific agreements with the owners (Apple Inc, for instance, for iOS based apps) to access their IP and licensing.

Web apps: have gained traction as a versatile and cross-platform solution. Web apps run within a web browser and do not require app store installation. Users access them simply by navigating to a website, making them platform-agnostic. An excellent choice for businesses looking to reach a broad audience without the constraints of app store policies, they can also be transformed fairly easily into independent apps for different target markets and experiences. Web apps are cost-effective to develop and maintain as they share a common codebase across various platforms. Popular examples include progressive web apps (PWAs) such as Pinterest.

Software development kits: crucial tools that offer developers the resources and libraries they need to create and improve their apps. Prebuilt code, APIs and documentation are frequently included in SDKs, which are essential for extending the functionality of mobile apps. The Google Maps SDK, for example, allows developers to smoothly incorporate mapping and location services into their apps, while the Facebook SDK permits easy integration of social media capabilities. The way IP is used in this scenario – where different technologies are integrated into a greater whole and offered as combined functionality or feature-rich apps – entails partnership and collaboration agreements, and SDK and OEM (original equipment manufacturer)-style licensing of the IP.

1.6. Conclusions

The world of mobile applications is in constant flux, with new areas, technology and trending apps emerging all the time. Staying ahead in this dynamic context demands not only keeping a careful eye on emerging trends, but also understanding how apps and

their related IP rights may be secured and used effectively. IP is critical to this process, serving as the foundation for safeguarding and commercializing digital assets.

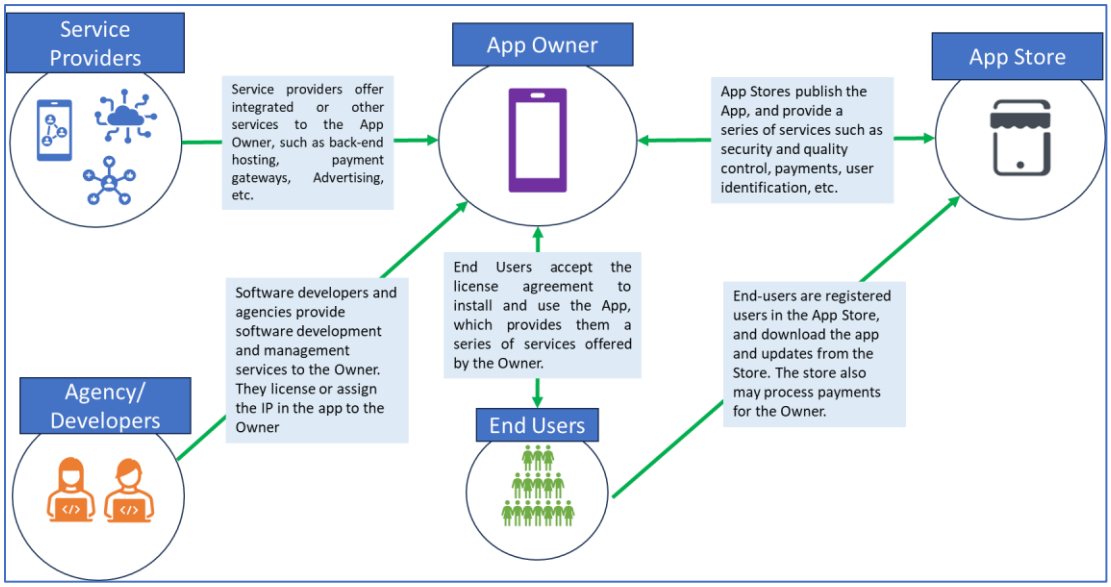
Chapter 2. The app ecosystem and key stakeholders

2.1. Introduction

This chapter examines the characteristics of the mobile application ecosystem, describing the environment and key stakeholders and the relations among these entities, providing an overview of various interests and concerns, while focusing on the developer's point of view, identifying hotspots and alternatives to deal with, reduce or mitigate them. In this manner, the reader will gain a better understanding of the actors, interactions and interests in the sector. It will also provide the context to define IP strategies, considering the interests and roles of the other actors. Chapter 5 will then examine the contractual relationships in more detail.

Throughout the life cycle of a mobile app – from conception to post-commercialization distribution activities – there is a vast array of stakeholders considered key to the success and sustainability of the ecosystem. As stakeholders, each of these parties contribute value and generate the synergies necessary for an industry that does not stop growing. In the analysis of the ecosystem, the roles, contributions and interrelationships of each of the key parties will be described, providing an overview that allows understanding and a systemic view of the mobile app industry.

Figure 2.1 Key parties in the mobile app sector



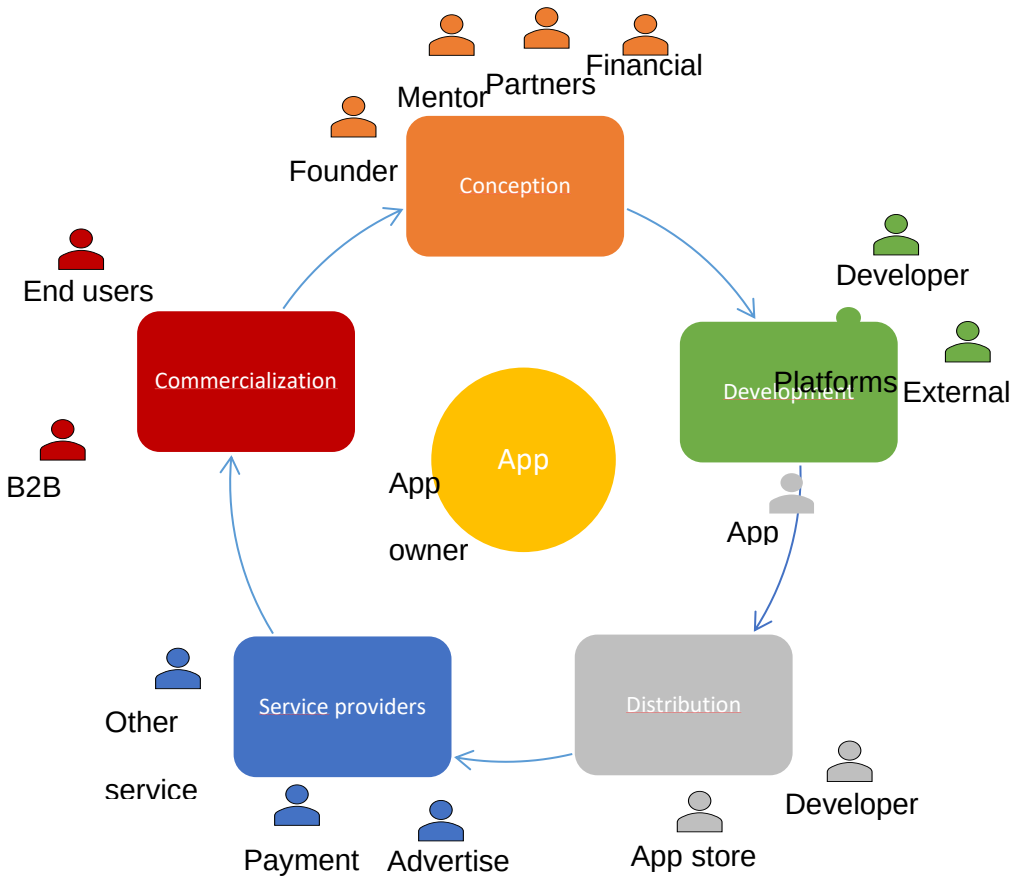
Source: Authors.

The key parties in the sector, illustrated in Figure 2.1 above, include:

- app owner;
- app developer and software development agency (agencies);
- platforms (operating systems for the mobile devices);
- app stores;
- service providers;
- business-to-business (B2B) clients; and
- end users.

These actors are not static but intervene at different stages of the mobile app's life cycle, from conception to commercialization, and the creation of new versions, in a cyclical manner. This is illustrated by the circle below, featuring the different actors who intervene in the different stages/phases of the app project.

Figure 2.2 Dynamic representation of the mobile app ecosystem and lifecycle

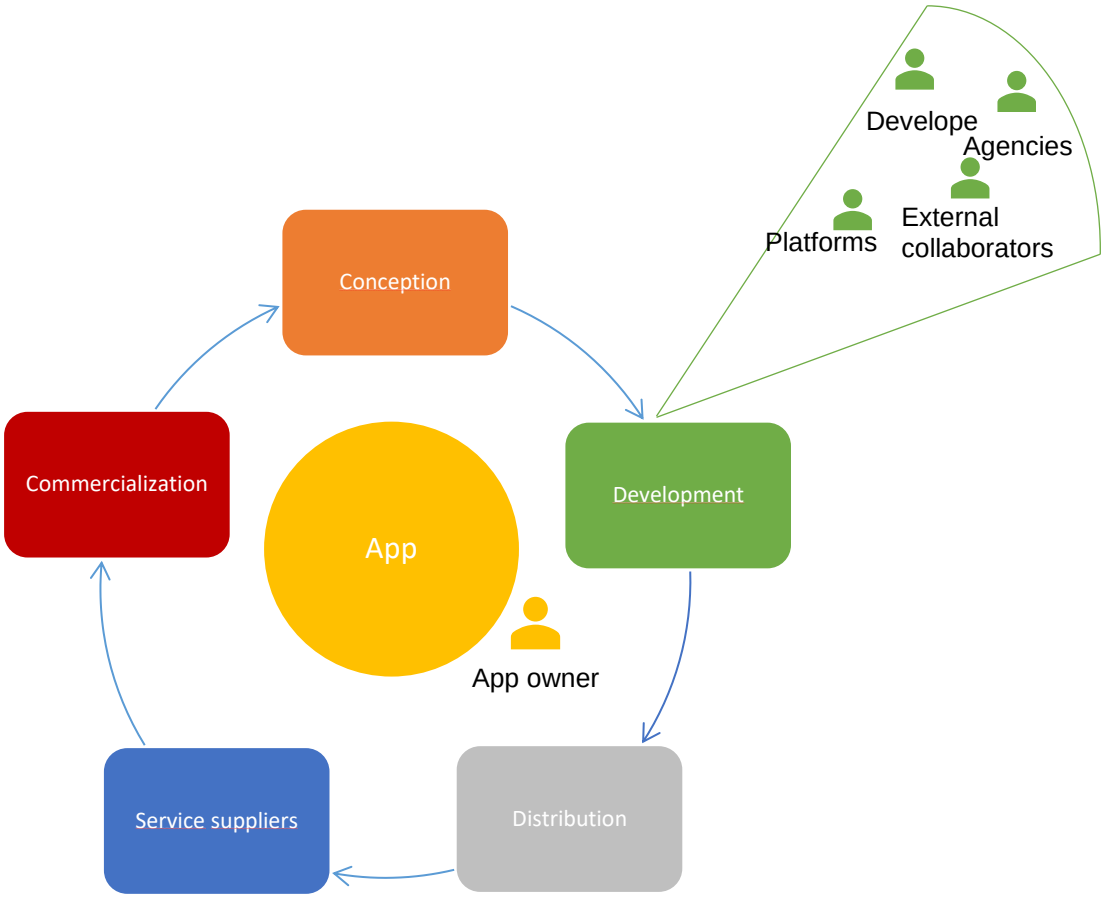


Source: Authors.

2.2. Conception and development stages

Key stakeholders in the conception and development phases include the app owner, developers/agencies and the platforms (mobile operating systems).

Figure 2.3 Key stakeholders in the conception and development phases



Source: Authors

2.2.1. The app owner

The app owner is the company or individual(s) that conceptualizes the mobile app. In the conception phase, they predefine the first idea(s) to satisfy the detected needs. The app owner is involved in all phases of the mobile app life cycle.

The app owner plays different roles and assumes several responsibilities to get a result that integrates the various specialties within the industry, including:

- **Mobile app conceptualizing**: the app owner is responsible for defining the mobile app's concept, identifying the needs/problems the mobile app aims to solve/fulfil, searching for relevant features, and establishing mid- and long-term goals.

- **Economics**: the owner responsible for allocating the necessary budget and resources for different phases of the mobile app life cycle. Includes searching and managing the funding for design, development, marketing and ongoing maintenance. App owners must ensure the project remains financially sustainable and healthy.
- **Overseeing the development process**: the owner is responsible for hiring developers or outsourcing the development work to agencies. The app owner usually participates as project supervisor, being part of a supervisory committee where technical decisions are made.
- **Strategic direction**: the owner is responsible for providing strategic direction for the project, often deciding necessary deviations from initial ideas.
- **Legal and contractual matters**: the app owner is responsible for addressing legal and compliance issues with advisers. Most refer to data privacy regulations, copyright and IP concerns.
- **Monetization**: the owner is also responsible for defining a monetization plan. The app owner is a relevant party to every business decision.

The app owner's contribution to the ecosystem

The app owner's contribution to the ecosystem includes:

- **Ideas and innovation**: app owners identify needs and gaps, and search for better solutions to address unmet needs.
- **Funding**: app owners, in pursuing funding and persuading different investment profiles, bring all their ability to inspire, guide, and bring their vision to life. This is based on their presentation skills and networking, allowing them to reassure potential investors.
- **Job creation**: the mobile app life cycle requires teams of professionals, including developers, designers, testers, marketers and advertisers. App owners, by initiating and running their projects, create job opportunities, thereby reducing unemployment.

- **Market expansion**: app owners, by means of internationality acceptable mobile apps, contribute to trade and export revenues, expanding market reach and economic growth.
- **Fostering community**: app owners, through mobile apps, promote community building, enabling individuals to foster connections, disseminate insights and engage in collaborative endeavors.

Interactions. The app owner interacts at all stages, and plays an essential role. They provide strategic vision internally, and balance the positions and weigh the roles, profiles and visions of project members. Externally, they safeguard the viability of the mobile app in the face of market and legal challenges. In the following sections, the specific interaction of the app owner with the other parties will be considered.

2.2.2. App developers and agencies

The app developer is the professional(s) responsible for designing, creating and maintaining apps tailored for specific platforms or devices, using various programming languages and tools. Developers must understand end-user requirements to design the mobile app's user interface, implement functionality, test the app in different environments, and deploy it to app stores or distribution platforms.

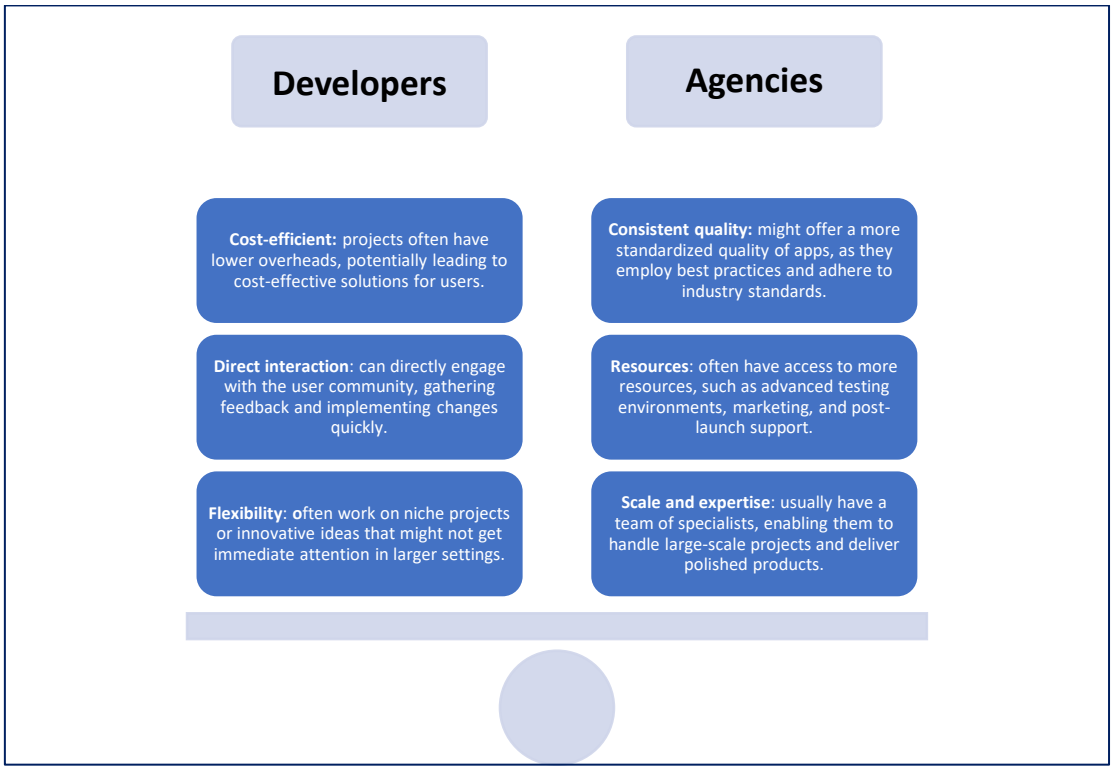
During the process, developers may be internal (inhouse) or hired as external developers, either as a freelance contractor or a development company (often called an agency/agencies), to build the mobile app. This also includes third-party developers who build technologies for other mobile apps to use (in software development kits, SDKs or software libraries), providing prebuilt functionality that can be incorporated in the mobile app. This technology will be licensed to the app owner. This activity, including development, integration and testing of the software, will impact on IP (see chapter 5)

During the development process, individuals in different roles and responsibilities work to deliver a result that integrates the specialties within the industry, including:

- **Mobile app developer**: responsible for programming and building the app. There may be sub-specializations such as iOS, Android or cross-platform developer.
- **UX/UI designer**: responsible for user experience (UX) and user interface (UI) design, ensuring the app is intuitive and visually appealing.
- **Software architect**: designs the overall structure of the application and decides on the most appropriate technologies and tools for development.
- **Business analyst**: works to define the requirements and ensures the application meets business or market needs.
- **Tester or QA** (quality assurance): in charge of testing the application at different stages to ensure its quality and find any bugs.
- **Project manager**: coordinates the team, sets deadlines and ensures the project progresses according to the established plan.
- **Other roles**: depending on the complexity and specificity of the project, other roles involved in app development include security and database specialists, among others.

These developers may be independent or work in agencies (see figure 2.4).

Figure 2.4 Contrasting individual developers and agencies



Source: Authors.

The developer's contribution to the ecosystem:

Developers' core contribution is technological innovation as they continuously expand the parameters of technological feasibility, culminating in novel and distinct app experiences.

- **Addressing end-user needs**: by developing apps that cater to specific user requirements, they enhance the usability and relevance of the mobile platform.
- **Economic contribution**: creation and marketing of apps contribute significantly to the economy, catalyzing employment opportunities and revenue conduits.
- **Educating end users**: through mobile apps, developers can spread knowledge, enabling users to learn new skills, access educational content and more.
- **Integrating technologies**: capitalize on avant-garde technological advancements such as AI, AR and VR to amplify application capabilities and cultivate superior user engagement.

Main interactions of developers with other ecosystem actors

Between developers and platform: During the conception stage of the app idea to the start of development, the developer (in-house or agency) must define the platform (operating system beyond the app) on which the app will be based. This will have an impact on the development process.

During the development stage, the interaction of the developer/s and the platform will be governed by the terms and conditions of the platform. Depending on the development environment, and the tools used, terms and conditions of the platform's integrated development environment (IDE), software development kits (SDKs) or application programming interfaces (APIs) may apply:

1. Official IDE for each platform application development, facilitates the development process, from creation to testing and debugging, and deploying the apps.
2. SDK, includes a wide variety of tools, such as device emulators, debugging tools and libraries needed to develop apps.
3. Available APIs, provided by platforms to develop specific features in apps such as location services, multimedia and connectivity.

From developer/app owner to app store: During the distribution phase of the mobile app (detailed below), the distribution channels must be defined by the app owner, taking account of the developer's considerations in terms of the technical impact of the decision. Here, app stores appear as a key party, given the relationship between developer and app store is governed by specific contracts established by each app store (see chapter 5).

App store agreements

The developer or app store distribution agreement and developer program policies define the terms of the relation between app owner and app store, including platform terms.

For Apple's App Store, the relationship is mainly defined by the developer agreements and App Store Connect terms of service that Apple offers for its content services, and other terms and conditions associated with the publication and distribution of apps. With the Google Play Store, the relationship is governed by the developer distribution agreement, which establishes the rules, terms and conditions the app owner must follow to publish and maintain their applications in the store.

2.2.3. Platforms

The term platform is often used to refer to the operating system of the app. Platforms are the software architecture that serves as a foundation for other programs or apps to run on. They usually include security features and procedural and software rules with which apps must comply in order to use the platform. When a developer decides to design an app, the platforms are the basis on which the app will run. Thus, this technology must be defined at the conception and development stages. Apps exist within a platform, with several popular platforms supporting apps on mobile and portable devices.

Currently, the Android and iOS platforms significantly occupy the mobile operating system market, accounting for an estimated 99 per cent of the total share. Android is at the forefront, with notable mobile device manufacturing entities, namely Samsung and Huawei, playing a pivotal role in fortifying its preeminent position.

Platforms market share, 2023

The largest platforms by market share of installed phones in the second quarter of 2023 were:

1. Android, dominating the market, with approximately 70.8 per cent of the global market share.

2. Apple iOS, Apple's mobile operating system, has a significant presence, with approximately 28 per cent.

Source: Statista, Global market share held by operating systems from 2009 to 2023, by quarter." *statista.com*. 2023. <www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/>.

The primary objective of platform operators is to augment their user base, which includes both individual users and app developers, and under certain circumstances also encompasses mobile handset manufacturers. It is imperative to acknowledge the symbiotic relationship between these parties, given app developers invariably gravitate towards platforms with the most end users, and end users seek platforms with a rich array of apps complemented by compelling hardware features.

Platforms' contribution to the ecosystem

Platforms provide an indispensable legal and regulatory infrastructure, such as:

- **Standardization**: facilitate a coherent and unified development framework, enabling the interaction of apps with various hardware under standard protocols.
- **Security and privacy**: establish security protocols, guaranteeing the protection of end-user data and integrity of the app.
- **Market accessibility**: platforms are matched by the corresponding app store, and through their app stores, act as intermediaries between developers and users, ensuring applications comply with legal and technical guidelines.
- **Compatibility and adaptability**: allow applications to adapt to various devices and hardware solutions, providing the end user with a uniform experience. Users are comfortable with a standard operating system where user experience is harmonized.
- **Updates and support**: provide regular updates to address emerging security and functionality challenges, ensuring adaptability and longevity of apps in the ecosystem.

Platform interactions

The relationships between platforms and app owners and developers are commented on in the previous section, highlighting the need for balance between the parties but often the platforms contract on standards terms that are usually more favorable to them.

Interactions between platforms and app stores. Platforms and app stores are intimately linked, particularly where the platform provider is also an app store, such as Google or Apple. Taking into account the two main platforms worldwide:

1. The Android platform interacts with several app stores such as Google, Amazon and Microsoft, but not the Apple App Store. In particular, Google Play is the widest app store in terms of available apps and downloads for Android (even considering China).
2. The iOS operating system interacts only with Apple App Store, which allows only apps developed under the iOS Platform.

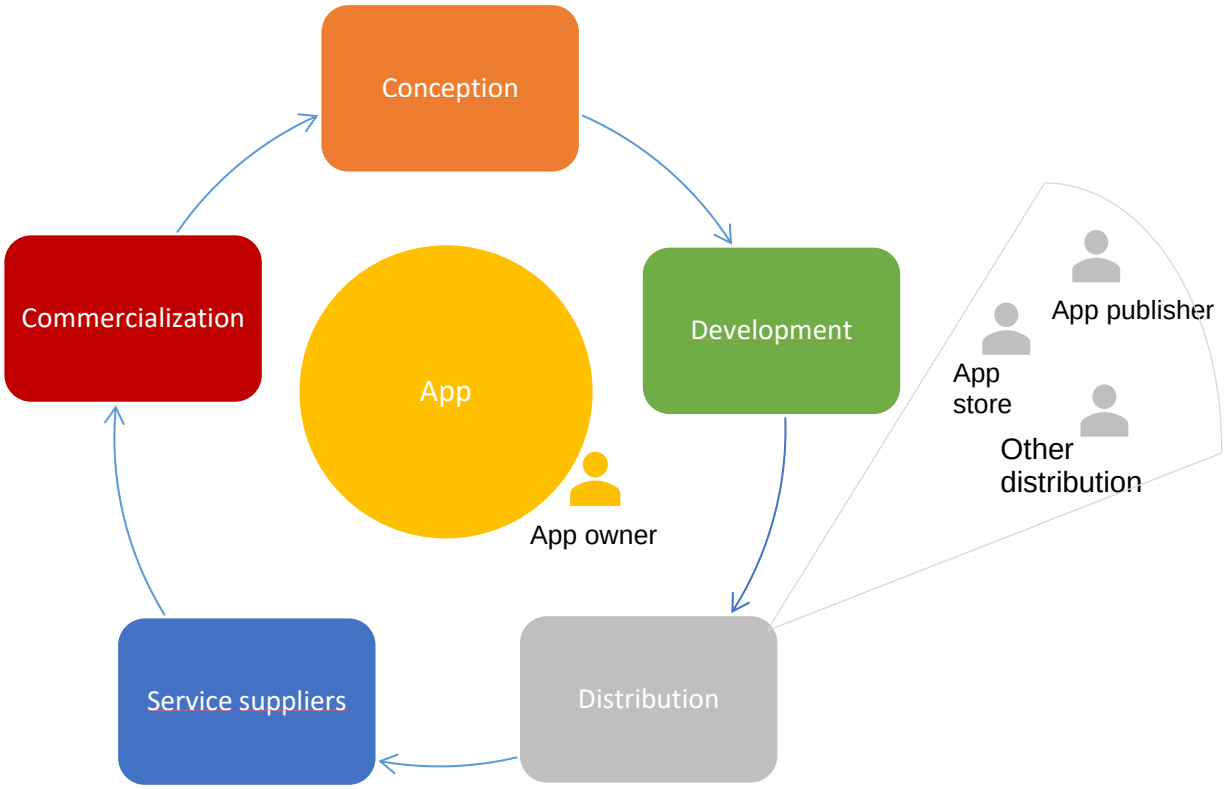
App stores interact with platforms mainly in the following manners:

- **App verification**: once an app is developed, it undergoes a review process before it is listed in the app store (for iOS) or Google Play Store (for Android). This is to ensure safety, compatibility and adherence to app store guidelines.
- **Update mechanism**: app stores also manage updates. When developers release a new version of an app, end users are notified, ensuring they have the latest, most secure and best-performing version of the app.
- **Security**: app stores have guidelines that developers must follow, ensuring apps do not pose risks to the system or user data. The platform then enforces these guidelines during run time, isolating malicious activities or ensuring end users privacy (or lack of).

2.3. Distribution: publishers and app stores

At the distribution stage of the cycle, there are further relationships to take into account that are commented here.

Figure 2.5 Actors involved in the distribution phase



Source: Authors.

2.3.1. The app publisher

App publisher is more a role than an entity, and often assumed by the app owner, though in some circumstances (where an owner has licensed an app to a third party for distribution, for example) it may be a separate entity. It is the role performed by the entity or individual responsible for publishing and bringing the mobile app to the market, handling its distribution (via the stores), and often overseeing marketing and monetization strategies. App publishers are responsible for submitting the app to app

stores but they often collaborate with developers to prepare all the necessary assets and documentation for the submission process.

App owners and publishers

It is important to note that in most cases the app owner is the app publisher, especially in smaller development teams or start-ups, where a single entity manages the entire app life cycle. In others, developers, agencies or other third parties take on the responsibilities of an app publisher, in particular, app store publishing and update tracking.

In larger organizations, these roles may be different, with dedicated teams or partners handling every aspect of the app journey, from concept to distribution. The benefits of having an app publisher's expertise will translate into benefits via enriching the ecosystem.

During development, distribution and commercialization, app publishers assume several responsibilities to obtain a result that integrates the various specialties within the industry, including:

- **Interaction with the app store**: app publishers are responsible for submitting the app to the app store and for handling the relationship with them.
- **Marketing and promotion**: app publishers are responsible for marketing and promoting the app to reach a wider audience. They may collaborate with the developer on marketing materials and strategies.
- **User feedback and support**: after the app's release, the app publisher collects user feedback, reviews and ratings. They work with the developer to prioritize and address user issues and improve the app.
- **Mobile app updates**: app publishers coordinate the release of updates and communicate with users about new features. They provide feedback for developers to enable work on updates and improvements based on evolving market trends.

- **Compliance with app store guidelines**: app publishers are responsible for being aware of app store guidelines and policy updates to prevent app removal or suspension.
- **Strategy collaboration**: the publisher can take responsibility for collaborating on the long-term strategy for the app, including potential expansions, new versions or spin-off apps.

The app publisher's contribution to the ecosystem

App publishers contribute significant value to the app ecosystem, including:

- **Market understanding**: they facilitate a coherent and unified development framework, enabling apps to interact with various hardware, under standard protocols.
- **Better dissemination**: they may have a global presence, helping apps reach international markets more effectively.
- **User acquisition**: have the ability to attract a larger user base through their marketing efforts and user acquisition channels, which can be challenging for app owners.
- **Compatibility/adaptability**: they allow applications to adapt to various devices and screen resolutions, providing a uniform experience for the end user. Users are comfortable with a standard operating system where user experience is harmonized.

App publisher interactions

Between app publisher and developer. The publisher and the developer have distinct roles, but need to interact in relation to publication and distribution of the app:

- The developer takes the lead in building the app, working on coding, design and functionality. They bring the app publisher's vision to life and ensure the technical aspects of the app are sound.

- The app publisher reviews the mobile app's progress and provides feedback to the developer. They may request changes, improvements or additional features, based on market research or user feedback.
- Developers conduct rigorous testing to identify and fix bugs and glitches and to ensure the app functions smoothly. The app publisher is involved in quality assurance to ensure the app meets expectations.

Between app publisher and owner. When the owner is not the publisher, these actors usually discuss and implement the chosen commercialization and monetization strategy, whether through in-app purchases, subscriptions, ads or other methods. They collaborate on integrating monetization elements into the app.

2.3.2. App stores

App stores are online marketplaces where end users can review and download apps to their devices. They have emerged in any market segment where software can be delivered online. They may be tied to a desktop operating system (Google Play Store or Apple's App Store, for example), a mobile platform (Google Play, iTunes, BlackBerry World, Microsoft Store), a browser (Firefox Marketplace, Chrome Web Store), a television platform (Samsung Apps, Iliad's Freebox), social networks (Facebook) or other platforms.

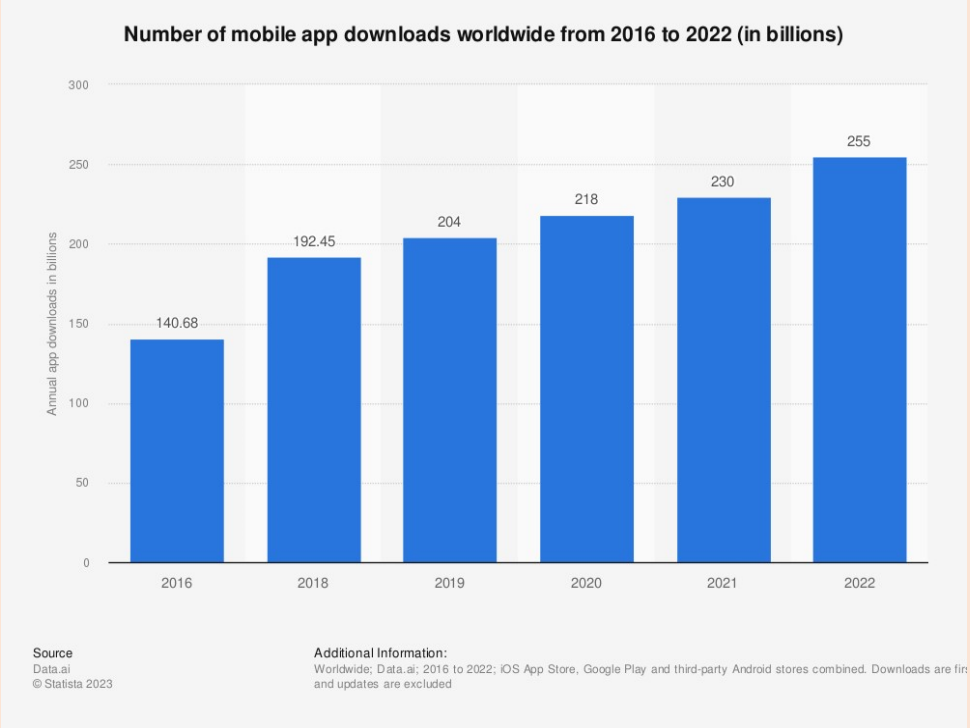
App stores' market positions

Google Play and the Apple App Store are currently the two largest app stores. According to Statista, in 2022 there were over a total 109.9 billion downloads on Google Play. During the third quarter of 2022, Google Play offered 3.55 million apps, leading the app store ranking of available apps. The Apple App Store was the second largest, with approximately 1.6 million available apps.

While Apple and Google are leaders with regard to downloads and revenue, there are other players with varying degrees of market success and relevance. The Amazon Appstore offers approximately 476,00 Android apps to audiences worldwide, with gaming, education and utilities apps the most popular categories. There are also several

third-party Android app stores in China, including the Tencent Appstore, which had 43,840 available apps in 2021.

Figure 2.6 Annual number of global mobile app downloads in billions, 2016–2022



Source: Statista. “Number of mobile app downloads worldwide from 2016 to 2022.” statista.com. 2023. www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/; and: “Annual number of app downloads from the Google Play Store worldwide from 2016 to 2022.” statista.com. 2023. <www.statista.com/statistics/734332/google-play-app-installs-per-year/>.

When deciding which app store is preferable, app owners, with the developers, will consider the platform’s potential for future growth and determine which best addresses their audience. Usually, developers build the apps for both Android and iOS platforms and all major stores.

Furthermore, for the app owner, the value of an app store depends on several factors, including:

1. the submission process;
2. levels of certification/quality control it enforces over published apps; and
3. flexibility in pricing mechanisms and promotion, and revenue-generating capacity.

The app store's contribution to the ecosystem

App stores are key and unavoidable players in the ecosystem and offer:

- Centralized platform for distribution: app stores provide a centralized platform for developers to distribute their apps, reaching vast numbers of potential users with ease, avoiding fragmentation.
- Standardized review processes: ensure that apps meet certain quality and security standards before they are made available to the public. This process builds trust and ensures the safety of users and their devices.
- Monetization opportunities for developers: **t**hrough in-app purchases, subscription models and advertising, app stores have introduced various monetization strategies, helping developers generate revenue from their creations.
- Support for a broad spectrum of apps: from games to productivity tools, and educational apps to fitness trackers, app stores support a variety of applications, catering to diverse user needs and preferences.
- Innovation and competition: the presence of app stores has spurred innovation, with developers constantly trying to offer unique and better products to stand out in the crowded marketplace.
- Ecosystem connectivity: app stores, especially those associated with specific operating systems such as Android or iOS, contribute to the broader mobile ecosystem. They often integrate with other system functionalities, such as voice assistants, cameras and other hardware features, enriching the overall user experience.

From 2020 onwards, there has been significant discussion about and changes in app store fee arrangements. As of August 2023, app stores take a (standard) 30 per cent commission for transactions and regular subscriptions, with some discounts.

Small business programs

More recently, to cater for small business and start-ups, app stores have reduced their fees for this segment from the standard 30%, including:

- Apple offering small app owners to pay a reduced rate 15 per cent commission on in-app sales in the Apple App Store.

- Google also halved their fees for in-app subscriptions for small businesses reporting earnings lower than 1 million US dollars, and these publishers could enroll in its 15 per cent service fee tier group.
- In June 2021, Amazon Appstore introduced its Small Business Accelerator program that allows developers with less than 1 million US dollars in revenue to pay just 10 per cent in commission fees.

A focus on app stores in China

China has one of the most extensive app ecosystems, with end users in the county engaging with an average 7.5 mobile apps per day and downloading approximately 52 apps every month.

The app market has been growing particularly fast. Google Play Store is not available in the country, though various Android stores have already launched, resulting in a fragmented app store landscape.

Among the players, the Huawei AppGallery held the largest Android app market share in China as of May 2022, with 44.31 per cent, followed by the Oppo Software Store, and the VIVO app store. At the end of 2022, the Huawei AppGallery counted more than 580 million monthly active users worldwide. Quick App, Huawei's development and distribution platform for lighter app experiences, counted 170 million active users per month.

Source: Statista. "App stores – Statistics and facts." *statista.com*. Aug. 30, 2023. <www.statista.com/topics/1729/app-stores/#topicOverview>

Interactions involving the app stores

The interactions between app stores and developers are detailed in the previous section.

From app stores to end users. An app store's terms of service (TOS) and the privacy policies that end users must accept when they first download a mobile app or use an app rule their interactions. These documents govern the use of the App Store, and even the use of apps, including, for example, how personal data will be used, stored and shared. Generally speaking, terms for end users set out the following clauses:

- **End-user conduct**: end users must follow the rules and regulations when using the app store, refraining from any malicious activities or attempting to bypass any restrictions.
- **Payments**: when purchasing any content, end users might be required to provide payment information and agree to certain financial terms.
- **Privacy**: the app store collects and uses personal data as per its privacy policy. This information can be related to user preferences, purchase history and usage patterns.
- **User-generated content**: some services in an app store allow end users to create and upload content. In doing so, end users grant the app store certain rights to display and distribute that content.
- **Limitation of liability**: the app store's liability for any issues arising from the use of the app store is limited, typically to the amount paid for the service causing the issue.

Example app store terms and conditions

The terms and conditions that govern the use of the Google Play Store for end users are referred to as the Google Play Terms of Service. More information is available on the Google website online at https://play.google.com/intl/en-US_us/about/play-terms/index.html.

The terms and conditions that govern the use of the Apple App Store for end users are referred to as the Apple Media Services Terms and Conditions. More information is available on the Apple website, online at www.apple.com/legal/internet-services/itunes/.

As from 2022, there have been new regulations in certain countries concerning the behavior and terms of app stores, and other platforms, the most salient being the European Union's Digital Market Act.[2]

The European Union Digital Markets Act

On September 6, 2023, the European Commission designated Alphabet (Google Play Store), Apple (Apple App Store), ByteDance, Microsoft, Meta and Amazon as "gatekeepers" under the Digital Markets Act (DMA).

Gatekeepers are platforms that have a significant impact on the internal market, serve as a way for business users to reach their end users, and enjoy (or it is foreseeable they will enjoy), an entrenched and durable position.

Gatekeepers will have to:

- allow third parties to inter-operate with their own services in certain specific situations;
- allow their business users to access the data generated in their use of the gatekeeper's platform;
- provide advertisers and publishers advertising on their platforms with the tools and information necessary to carry out their own independent verification of their advertisements; and
- allow their business users to promote offers and conclude contracts with customers outside the gatekeeper's platform.

Gatekeepers must no longer:

- treat services and products they themselves offer more favorably in ranking than similar services or products offered by third parties on the gatekeeper's platform;
- prevent consumers from linking up to businesses outside their platforms;
- prevent users from uninstalling any preinstalled software or app if they so wish; and
- track end users outside their (the gatekeepers) core platform service for the purpose of targeted advertising, without effective consent.

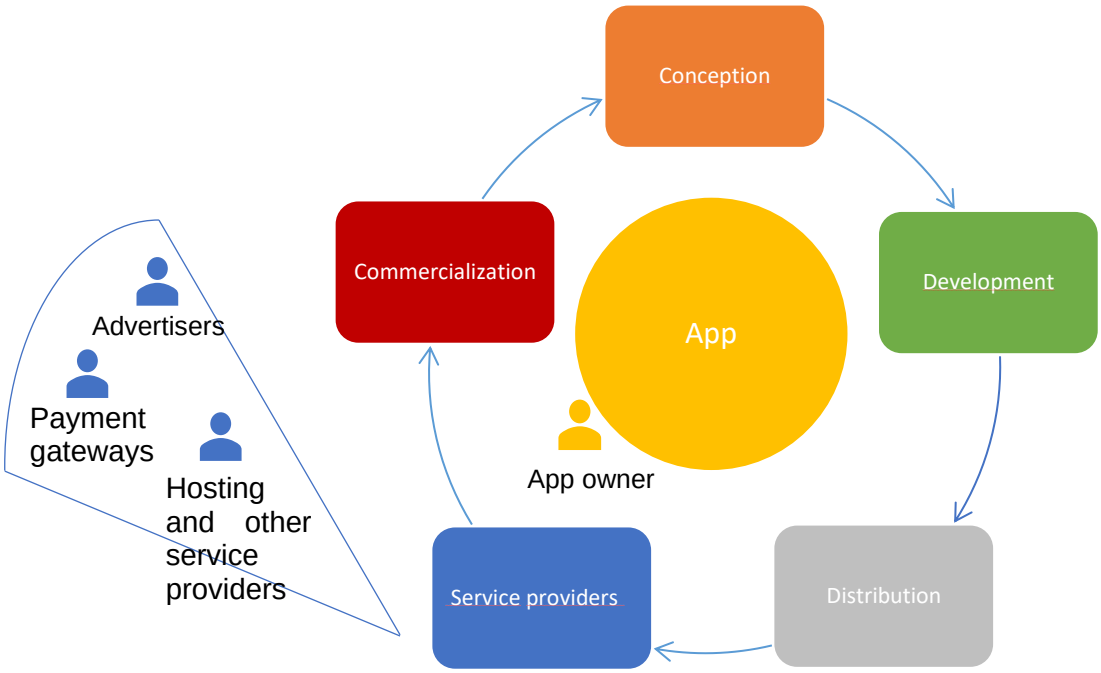
[2] European Union, European Parliament and Council. Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). EUR-Lex, 2022. http://data.europa.eu/eli/reg/2022/1925/oj.

The DMA will apply to basic platform services provided or offered by gatekeepers to professional users established in the European Union, or to end users established or located in the European Union. This is irrespective of the gatekeepers' place of establishment or residence, and of the law otherwise applicable to the provision of the service.

2.4. Additional service providers

The following extract of Figure 2.2 show the involvement of additional service providers in the ecosystem.

Figure 2.7 Additional services key parties



Source: Authors.

Mobile apps are complex technologies and offer a wide variety of features and services. In many instances, these features are not provided executed in the app itself, but are linked to the apps and executed in back-end / online servers, run by third parties who supply these features to the app owner.

2.4.1. Hosting services

A hosting service is the basic service that hosts the back-end of the mobile app for developers and owners, so their more sophisticated functionality can be served to end users (front-end apps), or can run and handle incoming requests from the mobile devices (backend apps).

App hosting is most commonly offered as a software as a service (SaaS) subscription, which allows developers and owners to run their applications on servers or in a cloud hosted by a service provider. This allows them to avoid high investment in building and maintaining the underlying infrastructure, enabling them to lower their costs by paying only for what they use, and enjoy upgrades in functionality and security, as well as easy integration with their existing data and systems.

Apps are built in different manners, with a variety of architectures, and many upload or require access to data from a server. These apps are dependent on this data and the backend server services, which also means that they cannot work without an active Internet connection. This may be problematic in some scenarios (at sea, in tunnels or mobile white spots). Many mobile apps that require user authentication, data sharing, streaming services or access to user-generated content will need backend hosting or content delivery services.

There are several hosting alternatives for the mobile sector, including:

- **Shared hosting**: this is one of the cheapest and easiest ways of hosting the app back-end, especially for smaller apps. For example, to make it simpler, an app developer can install WordPress on a shared hosting account and use it as a headless content management system (CMS) for the app.
- **Dedicated server hosting**: more resources available with dedicated server hosting than shared hosting. This will help developers build a backend that can

serve many users. The greater freedom and control, with root access to the server, allows the developer to build the app from the ground.

- **VPS hosting**: virtual private servers are those partitioned into multiple 'virtual' servers. System administrators are needed to work on the servers. This provides flexibility, security and full control over the hosting environment.
- **Cloud hosting**: one of the best approaches to hosting an app's back-end (server), as it is easy to scale, and the developer pays only for the resources used. Cloud hosting companies also tend to offer good server security.
- **Own servers**: app owners can buy their own servers and do the configurations. This works best for large-scale applications given it provides more control of the infrastructure. But this is expensive to procure, set up and maintain.

The hosting provider's contribution to the ecosystem

Hosting providers are essential to the ecosystem, providing the following contributions:

- **Scalability and performance**: provide scalable infrastructure that enable apps to manage varying levels of user traffic, ensuring optimal performance even during peak usage.
- **Reliability**: offer high availability and uptime, thereby minimizing downtime and ensuring, according to the corresponding service-level agreements, continuous accessibility for users.
- **Security**: frequently have robust security measures in place, including encryption, firewalls and intrusion detection systems, which help protect apps and user data from cyber threat.
- **Global reach**: many hosting providers have data centers in various regions of the world. This global presence may impact compliance with specific regulations, such as data protection laws.
- **Compliance**: hosting services adhere to industry standards and regulations, such as data protection laws. This helps mobile app developers ensure compliance with legal requirements.
- **Development and deployment**: offer tools and services for app development, testing and deployment, streamlining the development life cycle.

- **Cost-efficiency**: cloud-based hosting services allow developers to adopt a pay-as-you-go model, allowing remuneration only for the resources utilized. This ensures cost-effectiveness, particularly beneficial for start-ups and small businesses.

Choosing the right hosting service is a critical decision that can significantly impact the success of an app. Speed, uptime, security, scalability, support and pricing are key for decision-making. Making the wrong choice can result in slower loading times, frequent downtimes, compromised user data, and ultimately, a poor user experience**.**

2.4.2. Payment gateways

A payment gateway is the technology used by app developers and owners to integrate payment methods in their apps, particularly to accept debit or credit card purchases from end users or other means, including bank-owned wallets such as Bizum or even crypto wallets. Broadly speaking, the service interacts with the card-reading devices found in physical stores, and provides the payment processing functionality in online stores and apps.

These financial services (e-payments) give app owners, as merchant, access to various digital payment methods on their platform, including credit cards, Apple Pay or local payment options in a country.

The payment gateways' contributions to the ecosystem

Payment gateways are integral to ecommerce and gaming apps (where in-app purchases are prevalent), and offer the following features:

- **Facilitate transactions**: instrumental in enabling apps to process payments securely and efficiently, and of paramount importance for e-commerce applications, subscriptions and online services.
- **Increase conversion**: by offering flexible and secure payment options, make a significant contribution to reducing shopping cart abandonment rates, and fostering an increase in conversions within shopping applications.

- **Enhance user experience**: simplify the payment process, leading to a notable improvement in the user experience, which contributes to customer retention and loyalty.
- **Integrate advanced technologies**: payment gateways possess the capability to incorporate advanced technologies, such as AI, to detect fraud and augment transaction security. Refund costs are reduced and developers are provided with the relevant data for decision-making.
- **Globalization**: play a pivotal role in allowing mobile applications to expand their operations internationally by supporting multiple currencies and payment methods. This significantly broadens their reach and market potential
- **Security**: ensure the security of user financial data through rigorous measures, including encryption and strict compliance with established security standards such as the payment card industry data security standard (PCI DSS).

2.4.3. Advertising services

Advertising services are usually managed by an ad network provider that handles a portfolio of advertisers and serves adverts to end users via a variety of apps connected to the network. A network provider's reputation is essential to align app interest with the advertiser's portfolio; basically, matching end-user interests with products or services they might wish to buy.

Different types of advertising services are available for apps, including:

- **In-app advertising**: app owners can monetize their apps by displaying ads from ad networks or integrating their own ads. Common formats include banners, interstitials (full-screen ads that cover the interface of their host app) and rewarded video ads.
- **Mobile ad networks**: app owners can partner with mobile ad networks such as Google AdMob and Meta Audience Network to display ads within their apps and earn revenue from ad impressions and clicks.

- **App store optimization (ASO)**: involves optimizing app store listings with relevant keywords, and appealing visuals and descriptions to improve visibility in app stores such as the Apple App Store and Google Play Store.
- **Social media advertising**: app owners can use paid advertising on platforms such as Facebook, Instagram and X (formerly Twitter) to reach specific user demographics and promote their apps.
- **Location-based marketing**: leveraging user geographic locations to deliver targeted ads and promotions, which can be especially useful for location-based apps.
- **User data privacy compliance**: adhering to data protection regulations, such as GDPR, to safeguard user privacy when collecting and using data for advertising.
- **Performance analytics**: utilizing analytics tools to measure the effectiveness of ad campaigns, track user engagement and optimize strategies for better results.

Advertising services' contribution to the ecosystem

Advertisers are important for many app business models, and provide means for:

- **Monetization**: advertisement services serve as a pivotal revenue source for developers. Through the strategic display of ads within their mobile applications, developers have the opportunity to generate income. Many mobile applications, particularly those offered with no cost to the user, rely on ads to maintain the financial sustainability necessary for their development and continued operation. This practice ensures accessibility for users who may not possess the means to acquire these applications through alternative means.
- **Revenue diversification**: in addition to conventional methods such as direct sales or subscription models, apps can utilize ads as an alternative or supplementary income channel.
- **Targeted marketing**: advertisement services employ advanced targeting algorithms that allow advertisers to reach their specific target audience. This personalized approach delivers content that is not only relevant but also mutually beneficial to users and advertisers.

- **App discoverability**: in-app advertisements frequently serve as a promotional tool for other apps, amplifying their visibility and download rates. This fosters healthy competition and encourages innovation within the app ecosystem.
- **Support for smaller developers**: small-scale app developers, who may lack the resources required for elaborate marketing campaigns, find inclusion in ad networks instrumental. It permits them to compete on a more equitable and competitive level.
- **Data-driven insights**: ad services provide valuable data analytics capabilities, empowering developers to gain a deeper understanding of user behavior and preferences. This facilitates a continuous enhancement process.

2.5. Mobile operators

Mobile operators, also known as mobile network operators (MNOs), are considered a fundamental part of the telecommunications industry, as they provide wireless communication services to the app ecosystem. They manage the infrastructure and technology required for mobile communication.

Their role differs according to the degree of competition and development of communications networks in countries. In highly developed and competitive environments, mobile operators are frequently merely data carriers, though offer their own apps and services. In some countries with lesser developed markets for mobile operators (and sometimes a monopoly), these operators are more involved in the app market and may even charge percentages on transactions.

The mobile operator's contribution to the ecosystem

Outside of Wi-Fi, mobile apps cannot connect to the internet without mobile operators, who offer the following services:

- **Network infrastructure**: responsible for construction and maintenance of the physical infrastructure, which encompasses cell towers and base stations. This infrastructure facilitates connections between mobile devices and their networks.

- **Spectrum management**: undertake the acquisition of licenses for radio spectrum frequencies from competent regulatory authorities. These ensure the effective operation of their wireless networks.
- **Service provision**: offer various services, including voice calls, text messaging and mobile Internet access to their subscribers.
- **Roaming services**: many mobile operators have established agreements with counterparts in different regions. These permit their customers to make use of mobile services when traveling.
- **Billing and subscriber management**: take on the responsibility of managing billing processes, overseeing subscriptions and maintaining customer accounts in relation to the services they provide.
- **Investment in technology**: commit substantial resources to research and development endeavors to advance their network infrastructure, introduce innovative technologies such as 5G and enhance overall service quality.

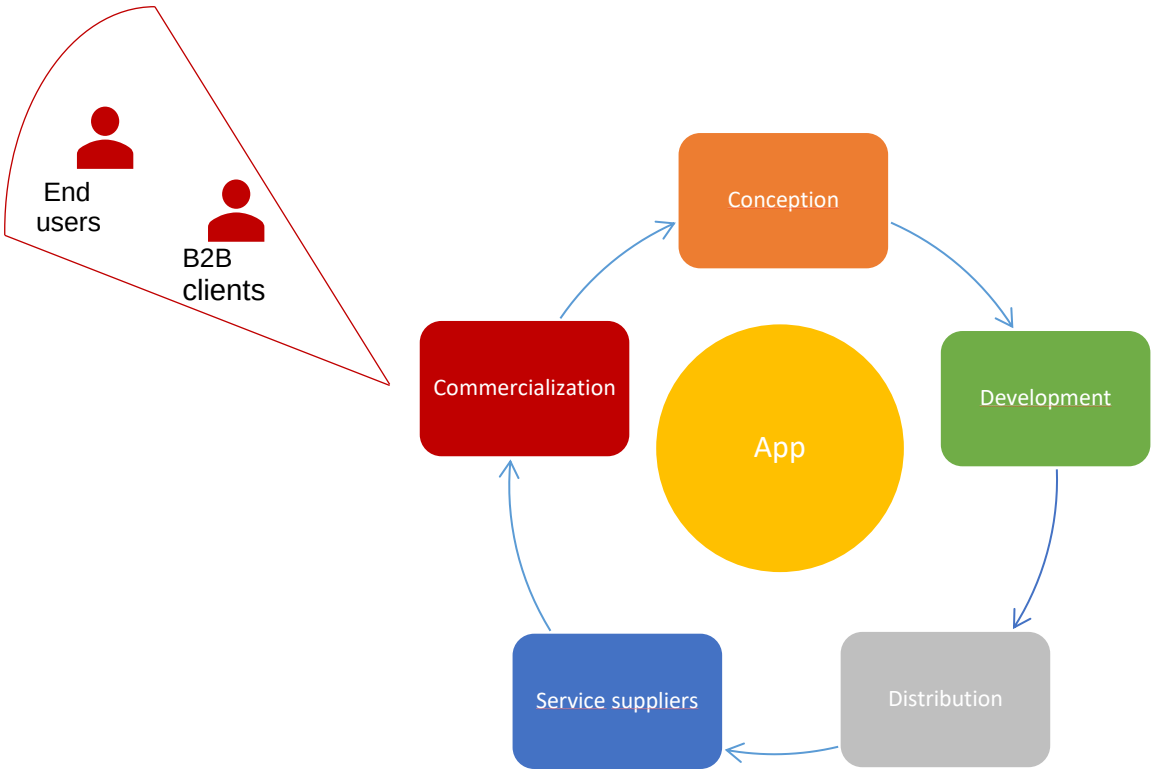
Mobile operators also build synergies with some mobile applications, particularly those of renown, to include them in their services. They offer service packages that include a subscription term and management through a dedicated app, a widespread promotional strategy. They also bundle other telecommunication-related services such as parental control, care for elderly persons, security and, increasingly, audiovisual content.

Their primary legal relationship is with end users who subscribe to their networks, but they often partner with app developers to promote and offer versions of the apps through their own platforms, offerings and app marketplaces.

2.6. Commercialization phase: interacting with clients

The final stage of the app cycle is commercialization, i.e. making commercial transactions with other business (B2B) and/or consumers (B2C: This is illustrated in - figure 2.8

Figure 2.8 Key parties in commercialization



Source: Authors.

2.6.1. End users

End user refers to the natural person or individual who utilizes a mobile app on a device such as a smartphone or tablet. They constitute the primary recipient of the app and employ it for purposes including but not limited to entertainment, productivity, communication and accessing information.

The end user engages with the app interface, performs actions within the app and utilizes its services or content. Their experience and satisfaction play a central role in the app's success. Developers strive to create engaging and functional user experiences that cater to the end-user's needs and expectations.

Further, the end user may provide feedback through reviews, ratings and comments on app stores, which often influence other users in deciding whether to download and use the application. Their active participation can contribute to the continuous improvement of the app and its success in the market.

Recognizing that the end-user's rights and data privacy are protected in certain national legal frameworks around the world (the most famous being the European Union's GDPR) is essential, to ensure a fair and secure digital environment (see chapter 8).

End users interact legally with several parties in the ecosystem, including:

- app owners through the app's terms and conditions or end-user license agreement;
- mobile operators, for telephone and data connection;
- platforms, when buying and installing a mobile device with a platform installed or purchasing apps or making in-app purchases processed by the platform; and
- with service providers such as payment gateways (app transaction) or even ad networks (clicking on ads in an app).

For more information on contractual relationships, see chapter 5.

End users' contribution to the ecosystem:

End users are the ultimate target and beneficiary of the app. For the app owner, they provide the following contributions to the ecosystem:

- **Feedback providers:** end users provide valuable feedback through app reviews and ratings. Developers use this to make improvements, fix issues and enhance user experiences.
- **Monetization**: in some cases, users contribute to the monetization of apps by engaging with advertisements or making in-app purchases. This revenue helps sustain app development.
- **Testing and quality assurance**: users, via their diverse devices and usage patterns, unintentionally assist in app testing, uncovering bugs and issues that developers can address in updates.
- **Data generation**: user interactions within apps generate data, providing developers with insights into user behavior. The data is used to refine app features and functionality.
- **Customization**: some apps offer personalization features, allowing users to tailor experiences to their preferences, contributing to a more engaged user base.

A Case study on interactions with end users: a game testing app

A European company provides game-testing services for worldwide videogame publishers, many of which publish their games as mobile apps on app stores. The testers are the end users. They provide essential feedback for conceiving, correcting and improving the mobile app, and thus, the game itself. In this scenario, the assignment of IP on tester recommendations for improvements is crucial and must be included in the terms and conditions. Further, nondisclosure agreements (NDAs) covering information revealed during game testing may protect the secrets of the game/app developer.

2.6.2. Business-to-business clients

B2B clients are those entities who are interested in the app, not as an end user but as part of their business activities. This model is often known as business-to-business-to-consumer (B2B2C), where the app owner grants rights to clients to use, include or modify a certain technology or product in order to offer another service or product based on the app to the market.

The key interaction of the B2B client is licensing a professional app to be used in its business (for example, visual recognition of spare parts for cars), or a consumer app that is published by the client and rebranded as their own (white labelling). The business client is thus an entity between the app owner and the end user, responsible for and managing the end-user relationship.

The business client's contribution to the ecosystem:

While many apps target consumer customers, there are more and more business app users, as apps become sophisticated end points and tools for business customers. These interactions provide:

- **Innovation in business models**: B2B engagement fosters innovation in business models. Platforms that facilitate B2B interactions in mobile apps

enable outbound open innovation, encouraging new approaches to conducting business and delivering value.

- **Digital transformation**: B2B users are at the forefront of digital transformation. They adopt mobile apps as part of their digitalization efforts, leading to improved customer experiences and operational effectiveness.
- **Demand for B2B app features**: B2B users' knowledge of the industry drives demand for specific features in mobile apps tailored to real needs. May include data analytics, customer relationship management (CRM) integrations and supply chain management tools.
- **Supporting start-up ecosystems**: B2B drives startups, contributing to growth and development of the ecosystem, particularly in the context of digital innovation and entrepreneurship. By incorporating developed third-party technology, and using the flexibility and innovation of developers, they generate a synergy that benefits the entire ecosystem.
- **Ecosystem collaboration**: B2B users, particularly in industries such as banking, collaborate within app ecosystems to cater to small and medium-sized enterprises (SMEs), facilitating financial services and support for this segment.

Case studies on apps for business client

An African mobile app provides services based on a white-label license. It is a ride-hailing and transportation app that operates in several African countries, including Algeria, Morocco, Senegal and Tunisia. The app offers on-demand transport services similar to popular ride-sharing platforms. The app owner provides the technology and platform as a white-label solution to local entrepreneurs or transport companies – the business clients or publishers – so they can license the platform and rebrand it under their own name.

A European company incorporates a third-party app, licensed as a white label to provide quasi-financial services such as money transfers and data top-ups for Internet browsing in Benin, Burkina Faso, Cameroon, Chad, Côte d'Ivoire, Gambia and other countries. The business user focuses on its expertise, especially on the ground, understanding local needs, and licenses the application technology from the app developer.

2.7. Conclusions

The mobile app ecosystem possesses a sophisticated and complex structure. While some parts of the system show a higher level of atomization, with many actors and types of relationships, particularly relating to service providers and app developers/owners, others are more concentrated, such as app stores. However, the general trajectory is one of constant expansion, as personal and commercial interactions become increasingly digital, and mobile apps provide essential connectivity and customized features on smaller devices (avoiding heavy laptops or personal computers). Each participant increases the overall vitality of the ecosystem, providing solutions and alternatives to any difficulties that arise.

An important aspect that emerges is the fundamental role of IP management in this ecosystem. Managing IP is not a peripheral element but is fundamental for promoting and defending creativity; IP rights arise out of creative activities and are the basis for safeguarding that innovation, facilitating the licensing of rights and their subsequent transfer. A thorough understanding of these aspects is indispensable for good IP management, which acts as a bulwark against potential legal infringement and is the backbone of sustainable business growth and enterprise development. This is looked at in detail in subsequent chapters.

Key takeaways: the main parties and their responsibilities in the ecosystem

- The mobile app ecosystem is varied and complex, with several key actors playing complementary roles in developing and providing apps to end users.
- It is important to understand the role and interests of these actors in order to act and evolve in this sector.
- IP is a core feature of this ecosystem. Protected by IP rights, each actor brings their own creativity and innovation to the sector, and leverages this IP to take their place in the market.

- Some actors have greater leverage than others, in particular the app stores. Understanding their role is key for app developers and owners to enable them to fully participate in the system.

2.8. Useful links and resources

Statista market data:

- www.statista.com/statistics/734332/google-play-app-installs-per-year/.
- www.statista.com/topics/1729/app-stores/#topicOverview.

European Union Digital Markets Act:

- www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC.

Google Play terms of service:

- https://play.google.com/intl/en-US_us/about/play-terms/index.html

Apple Media Services terms and conditions:

- www.apple.com/legal/internet-services/itunes/.

Chapter 3. Income streams in the app industry

3.1. Introduction

This chapter examines the diverse income streams available and used in the mobile app sector, and ties these with IP. A general overview is provided on alternatives, pathways and strategies to align protection and IP exploitation for the business models and income of actors in the mobile app sector, primarily app owners but also the many other actors such as advertisers, platforms and data providers.

This is not the place for a financial and economic analysis of income streams in the app sector, but a specific look at the relationship between IP and income. For the different revenue models, IP plays a different role, which may raise different issues. After briefly reviewing the revenue models, the second section of the chapter addresses how IP can be used as a mechanism to provide monetary value to an app venture, and to eventually attract investors and mitigate income worries.

After presenting several of the business models used in the mobile app sector, the focus will be on two key areas:

1. **IP-related income streams**: the basic issues surrounding IP and income in the mobile app sector will be considered, and the strategies and difficulties that may face developers and owners analyzed. This concentrates on licensing revenue for developers, owners and relevant service providers, and other actors in the sector monetizing IP (content, data, IP-related services).
2. **Other streams**: monetizing IP is not the only revenue stream for apps, with many income streams related to other financial models, including in-app purchases, subscriptions, advertising, sponsorship and partnerships, and, the biggest of them all, app store revenue share.

For related information on the economic aspects of mobile apps and IP, see chapter 7.

3.2. App business models

The different players in the mobile app ecosystem have been discussed, including software agencies who develop code; app owners who publish and manage the app itself; platforms, both technology platforms for operating the app, particularly the back-end, and the app stores as online marketplaces for publishing and distributing the app; service providers of all types; and, of course, end users.

Each of these actors has their own business model, based on technical and also commercial offerings. A key example is the app stores who offer a technical platform for uploading, managing and distributing the app versions, but commercially include significant services such as quality control, in-app payment procedures or advertising (and charge the app owner for this). When the app store also owns the technology on the mobile device (such as Apple), or provides operating system technology for that device (such as Google), then the platform's business model is multifaceted and there are many income streams.

Some numbers representing the app market

The following statistics illustrate the activity of the app market:

- Total revenue in the app market was projected to reach 522.70 billion US dollars in 2024.
- Total revenue is expected to show a compound annual growth rate (CAGR 2022–2027) of 8.58 per cent, resulting in a projected market volume of 755.50 billion US dollars by 2027.
- In-app purchase (IAP) revenue in the app market was estimated at 149.90 billion US dollars in 2023.
- Paid app revenue in the app market was estimated at 5.25 billion US dollars in 2022.
- Advertising revenue in the app market was estimated at 315 billion US dollars in 2023.

Source: Statista. "Statista market insights." *es.statista.com*. March. 2024. <www.es.statista.com/outlook/dmo/app/worldwide>. And Business of Apps "In-App Purchases". March 2024. < https://www.businessofapps.com/guide/in-app-purchases/>

Here, the focus is mainly on the mobile app itself and the IP associated with it, and those involved in developing the technology, preparing it for distribution and commercialization, and operating the app services for end users.

The main business models for the app owner are:

- **Paid apps**: this model consists in selling premium (i.e. non free) mobile apps for a price to be paid on the app store. This model entales mainly an IP license from owner to user, to enable the latter to download and use the mobile app, and the app owner to obtain revenues from this, in many cases minus a transaction fee from the app store.
- **Freemium models**: in this model, a version of the mobile app is available for free, while apps with more sophisticated functionality (or less obligatory advertising) are available for a price.
- **Additional in-app services**: in this case, the mobile apps with full functionality are totally free, and the owner's business model is based on generating revenue through other means, including
    - in-app purchases, where the app owner gains income from selling items, subscriptions and upgrades, among other things, through the mobile app;
    - in-app advertising (interstitial, banner, video, native or text advertising); and
    - affiliate linking and referrals where revenue comes from a third party.
- **Product and service sales**: many mobile apps are also freely downloadable, with revenue for the app owner coming from the sale of its own or third-party physical goods or services in or through the mobile app. For example, free banking apps enable income from financial services offered and carried out through the mobile app (micropayments, loans, transfers, insurance and investments, among others). For real world product sales, the most well-known are the online marketplaces (Amazon, AliExpress, MercadoLibre) and online

stores, but there are many mobile app-based marketplaces in specialist sectors. These include medical supplies, agriculture, fisheries and machine spare parts, where the app is used as an advertising, information and sales tool for identifying and selling real world products and services, with no IP commercialization really involved.

- **Subscriptions**: the app owner offers mobile app-based services on a recurring monthly or annual basis, which renew until they are cancelled by the owner or user. This generated revenue is a key factor for success and in obtaining finance. It is often the case for newspaper subscriptions, technical services such as storage or additional features on the app, and parental control.
- **Advertising**: probably the greatest source of income from third parties. The competitive dynamics of the mobile app space mean that many apps have to be offered for free, and app owners need to look to other sources of income. Advertising commissions make up a significant proportion of the mobile app income and advertising revenue supports many free apps (from social platforms to travel recommendations, to games, such as instrument tuning apps) that would otherwise be paid for.
- **Licensing**: some mobile apps or app technologies can be aggregated or embedded with other technologies and apps to create a more sophisticated or complete mobile app service for end users. These are often 'background' technology apps, such as visual or sound recognition, keyboards, security or other technologies that can be licensed to other app owners.
- **Other sources:** app developers have been inventive in looking at how to make money from mobile apps, finding multiple sources of income from their technology. For example, collecting and selling data generated by mobile app usage (often problematic when the data is user-related due to privacy regulation), or sponsorships.

These models are not mutually exclusive, and app owners often combine models to maximize revenue. Key aspects of these models are summarized in table 3.1 below. More information is available on the World Intellectual Property Organization (WIPO) website, www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo-tool-financing-mobile-apps.pdf.

App developers (including contracted software agencies) are more focused on monetizing their IP through licensing or assigning IP rights in their mobile app-related technologies and the code apps they develop for app owners, and also on offering essential maintenance and support services as well as sometimes managing the whole technical publication and operation of the app on the owner's behalf.

The next section considers the IP-related aspects of these income streams and looks at non-IP based revenue. These are not mutually exclusive, and many successful mobile apps combine a variety of IP-based revenue (royalties, licensing of content or data) and non-IP features such as advertising or premium device features.

3.3. IP-related income streams

A primary principle of IP is to give exclusive rights over creations and innovations to provide creators and owners of the IP with the opportunity to commercialize those creations and obtain income (though this is not the only purpose of IP). This mechanism is highly relevant to obtaining income from IP in apps. Thus commercializing IP can be seen as the process of bringing IP to the market in view of future profits and business growth.

To leverage this, an app owner or other actors in the sector should identify the IP assets that are generated around their mobile app or platform and how these can be used as a basis for commercial income (monetization). For leveraging IP in apps for funding opportunities, see chapter 7.

3.4. Relevant IP assets

What are these key IP assets? There are a significant number that can be considered, and each may have one or several commercialization opportunities:

- **Inventions**: embodied in app technologies (and related areas, such as platforms and communications, among others). These may be protected by patents or trade secrets, and there is the opportunity for inventors to monetize these patents through licensing or assigning the IP to third parties interested in using the invention for their mobile app.
- **Software code**: the main technology of a mobile app and the back-end platform, which is mainly protected by copyright (and trade secrets). This offers an opportunity for licensing the software to third parties (for example, keyboard technology licensed to an app for specific sectors such as education or health) or straightforward assignment (for example, assignment of a new mobile app from an agency to the app owner).
- **Content**: music, videos, images, icons, emojis, graphic designs; the mobile app world is full of content, and mobile apps are a key channel for commercializing the IP in this content through licensing or assignment.
- **Designs**: mobile apps include graphic designs, mainly in the user interface, and these can also be protected, and licensed or assigned to an app owner to use in their mobile app.
- **Data**: mobile apps generate a significant amount of data, or can be specifically used to collect various types of data: personal data of the person using the app; scientific, technical, or commercial data regarding sales or relationships generated by the mobile app; and metadata about mobile app usage as a whole. This data can be analyzed, or the statistical data extracted, and licensed or sold to third parties interested for their own business purposes.

- **Brands**: while the mobile app's own brand will not generally be a useful income-generating opportunity for the app developer – it is significant for defending the app's commercial value, and the trademark owner – once a brand has significant value, licensing its trademark rights to third parties, for them to be able to profit from the value for their own purposes, is an important revenue stream.

For how these assets can be protected by IP rights as a first and essential step, and the relevant protection mechanisms and rights generated, see chapter 4.

The next step is to identify how to generate income from these IP assets. This entails identifying the value of the assets for the business owner (app owner for the app, platform owner for the app store or back-end server infrastructure) and for third parties, and bringing and offering that value to the market. This entails defining the business model(s) of the mobile app, and building the offer of products and services around that value.

3.5. IP-related income generating models

It is necessary to drill down on how income may be obtained, through these different commercialization channels or models, for the different IP identified above.

Table 3.1 Key aspects, business models for the app owner

IP asset	Protection	Value	Commercialization	Income stream
Technical invention embodied in mobile app or platform	Patent, utility model	Special technical innovation providing solution and/or competitive advantage	Assignment Licensing for manufacturing, commercialization, and use	One-shot payment or deferred revenue Licensing one-shot or recurring royalties
Software code of app technology or mobile app itself	Copyrights, trade secrets	Functionality of mobile app, performance, security, etc.	Assignment Licensing for reproduction, distribution and transformation	One-shot payment or deferred revenue Licensing one-shot or recurring royalties

			OEM licensing to other app owner	OEM licensing (revenue share or fixed or variable royalties)
Content (music, videos, designs, images, icons, avatars)	Copyrights	Unique creation, recognition (music, images)	Assignment Licensing for reproduction, distribution or communication within the mobile app	Royalties or fees per use of the content, subscription fees
Data	Database rights, contractual protection or trade secrets	Business intelligence, user profiling, trends, etc.	Sale or licensing access to database	One-shot or recurring subscription revenue
Brand	Trademark	Singularity and distinction in the market	Licensing trademark for use in commerce	Usage fees

Source: the authors.

3.5.1. Commercializing inventions: patents

Patents cover inventions of a technical nature. They are prevalent for mobile device hardware and for communications protocols, but less so for mobile app software applications and their software-based functionality. An invention in the mobile app sector can generate income through assigning or licensing the patent rights to hardware manufacturers (who may want to implement the invention in the mobile device or software that runs the device, such as touch screen technology, scrolling, hardware-based authentication and security mechanism, or data management), or, if it is a software-implemented invention, to software developers who need to embody the invention in the mobile app itself:

- Assignment of patent rights, basically selling the patent to a single entity, is often the case when the assignee (purchaser) is accumulating key IP for new hardware or communication technologies (think of the 5G patents). These entities generate

large portfolios of patents to protect their manufacturing processes and hardware designs and devices. A patent holder who assigns the patent will usually negotiate a one-off transfer fee or have a mix of fixed payment and variable deferred payment over time or for when the invention (often at proof-of-concept stage) is validated for commercial exploitation.

- Through licensing, the patent rights holder offers the same rights to those who want to implement the invention in the mobile device or app (and if the patent/s are essential for a standard, may have the obligation to do so), with the opportunity to have multiple revenue streams from the different licensees.

For presentation and comment on the contractual aspects of licensing and assignment, see Chapter 5.

3.5.2. Commercializing Software: copyrights and trade secrets

Mobile apps are principally made up of software, and licensing or assignment of the copyrights in the software – directly to a user or indirectly through a third-party software developer or platform – is the principal revenue source for software agencies, app developers and owners, and mobile app-related platforms.

- **Assignment**: agencies often assign the mobile app they develop to their clients, the app owners, who become the copyright holder of the mobile app. The app can then be distributed by the owner, and when an assignment takes place, the app owner usually assumes future evolution and maintenance of the software. The app is often a complex work with many subcomponents often under open-source licenses (see chapter 8) and it is important for both the assignor and assignee to ensure compliance with their licensing terms. For further information on the contractual relationship between agencies and app owners, see chapter 5.

- **Direct licensing**: the most common method of distributing a mobile app is through licensing it to end users; that is, a license to download, copy, install and use the mobile app. The revenue from this licensing is mainly a single up-front payment, or a subscription to the mobile app or the mobile app combined with a service supported by the mobile app (data storage, parental control, security protection, gaming, among others). This licensing may also be for free (or freemium), as the copyright owner obtains revenue through other mechanisms such as advertising, referrals and sales of other goods and services. Under a freemium model, the app owner offers a free basic service and sells subscriptions for more advanced features or greater amounts of data, and other things.
- **Indirect or OEM licensing or technical partnerships**: many start-ups and smaller companies, as well as large corporations, create innovative software components such as authentication mechanisms, interfaces, device management features, security protocol implementation, keyboards, visual recognition functionality and data management, which are often built into and licensed as software libraries or software development kits (SDKS). These provide the building blocks for the app owner to create their mobile apps more quickly, with more features, and in a modular and sustainable manner. The library or SDK licensor's revenue comes from royalty fees for access and use of the SDK, or could be revenue share from downstream licensing of the mobile app that uses the SDK.[3]

Examples of app income streams

Mixed end user and business SDK licensing: A small company from the United Kingdom makes a smart keyboard mobile app. It is directly downloadable by end users and is also offered as an SDK to other app owners who want to use the features of the keyboard for their own purposes (tracking, advertising, user interaction, for example).

[3] A 'free' developer license is often provided for the app owner to build the app and test the technology prior to commercialization.

The keyboard is licensed directly to users for a subscription or single payment fee, and the SDK is licensed with a revenue share agreement with the other developers.

Parental control or online behavior monitoring: provide mobile apps and platforms for parents to monitor the use of mobile devices by their children. The company licenses the mobile app's software for free, which can be installed on several devices, but charges a monthly fee for the platform service that analyses use of the device, connected websites and other activities of the children. The income stream is recurring monthly revenue from the parent subscriptions to the service as a whole.

Meetings going online, supported by mobile apps: a small business in Spain provides a mobile app for securely connecting to formal company meetings (shareholders or board meeting, for example) and keeping certified records of member participation and voting. The mobile app is offered for free to end users (shareholders, board members), but the company pays a monthly flat rate subscription or a variable fee according to the number of meetings and participants, for access and use of the platform.

3.5.3. Commercializing Content: copyright and design rights

Mobile apps are becoming a main gateway to audiovisual, sound and other content. Spotify, Netflix and Roblox, among others, are not just web platforms but also have their own apps for accessing content. Law firms launch their own mobile apps to provide clients with access to news, model documents or advisories. Revenue comes from the content itself, which can be under pay-per-view/hear or subscription models, where the end-user license agreement sets out usage terms and payments required.

While these large platforms are the most visible tip, there are significant numbers of creators, design studies, musicians and artists who contribute new and creative content and designs to both mainstream and new mobile apps, including avatars and 'magical swords' for gaming, background music for promotional videos and adverts, icons and emojis. While the protection regime differs slightly between copyright and design rights, their use in terms of income streams is similar.

- **Licensing**: mass market end-user content (music, audiovisual works) is nearly always licensed on a subscription or pay-per-view basis, with the income coming directly from the end users. Also, creative agencies designing graphical interfaces, icons, fonts and other reusable creative elements will license their works to the app owner for one-off fees or recurring subscriptions. Other content providers such as news platforms will provide and license their content – often premium – on a periodic subscription basis, not unlike distributing newspapers to monthly subscribers. In particular, music labels and other players in the music industry will license their works to mobile apps and app platforms (Roblox, Spotify) either directly or through management entities (collecting societies) for block fees, per subscriber or per download/streaming.
- **Assignments:** rare in relation to content such as texts, music and artistic works, except when these are created specifically for an app owner for their exclusive use in or through the mobile app. For further information, see chapter 5.

3.5.4. Commercializing Data: data rights, trade secrets

Data has increasing value in today's connected and digital society, and mobile apps are a huge source. Data are fundamental for targeted advertising, market research, business intelligence, and new machine learning and AI-based technologies and businesses. Not all jurisdictions protect data or databases in a specific manner (see chapter 4) but protection is usually afforded through trade secrets. Thus, collecting, verifying, managing and providing access to data is a potential income-generating activity and curating it becomes essential. Monetizing this data presents an opportunity for the app owner and other actors who have data relating to the mobile app sector (in particular, platforms and app stores).

There are a variety of datasets in the mobile app sector that may be of specific interest when generating revenue, including:

- **User data**: mainly how the app is used and what activities are carried out with it. This data is often regulated personal data, and subject to strict controls, including to whom it may be disclosed and for what purposes it be processed (see chapter 9). Monetizing this can also be difficult due to regulatory restrictions but the data can be anonymized, aggregated or otherwise adapted and thus commercialized in some manner.
- **Scientific and technical data**: many mobile apps are used for scientific or technical purposes, or they generate technical data on the environment, society as a whole, and transport, among other things. This data is not regulated like personal data, and the opportunities for commercialization and income generation are greater, or at least simpler to manage.
- **Commercial data**: often a core feature of mobile apps, to process commercial data for clients. This can be accumulated by the app owner and, depending on the agreement with users, could be a source of further income if aggregated as statistical data for business insight or intelligence.

In terms of exploitation and income, access to datasets for commercial purposes (with or without transfer of the dataset to the licensee) is usually granted to third parties under a licensing scheme on an exclusive or nonexclusive basis. This can be on through subscription if the datasets are updated. Conditions of the licensing can include the fields of use and restrictions on what may be done with the data; for example, some scientific medical data may not be used for diagnostics.

3.5.5. Commercializing brands: trademarks

Trademarks are used in a variety of ways to generate income in the mobile app sector. Primarily, recognized brand owners leverage their trademarks to sell the device hardware and mobile apps, and to increase brand reputation and recognition for better placing in app stores and other rankings. However, at the mobile app level, business-to-consumer (B2C) apps usually want to sell recognized third-party branded products, while

B2B apps want to include recognized branded technology or services in their offerings (think of Intel® Inside and Android® compatible, or the value of Amazon® for the AWS infrastructure services). So, entities that create technologies, content and services for the mobile app sector that build a high recognition and reputation can monetize their brand, in collaboration with the mobile apps and platforms.

Vis-à-vis income, trademarks are rarely if ever assigned. The main revenue stream is licensing, under strictly controlled terms that protect the brand and brand owner, while permitting use of the trademark by a third party against a royalty payment or fee.

An IP Checklist: identify monetizable IP and associated income streams

The first step in monetizing IP is identifying the assets that you may have and the rights that cover those assets:

Inventions:

- Have you created an invention and is it protected by patent rights?
- Are you going to use your invention yourself, or license it to third parties, under an exclusive or non-exclusive license?
- Is a third party interested in purchasing the patent rights (in whole or part/territory/field of endeavor) on an exclusive basis?

Software:

- Have you developed software for a mobile app (or have you engaged a third party to do this for you)?
- Has this been developed under exclusive arrangement for the benefit of a single client, or is this independent research and development, creating an asset for your company?
- Is the technology usable in a variety of scenarios and licensable to several different parties?
- Are there any third parties interested in acquiring all the IP rights, for a complete assignment of IP to them?

Content:

- Have you developed copyright protected works (text, images, audiovisuals, music and sounds, designs, among others) for your mobile app?

- Are these materials exclusively for you (or a single client), or useful for and usable by a variety of people who may be interested in licensing them from you?
- Is it interesting or useful for you to take advantage of content intermediaries (collecting societies, image banks, online repositories) for commercializing the content and monitoring compliance?

Data:

- Does your app collect or generate data?
- Is this data regulated under personal data laws? If so, do you have appropriate legal basis (including, for example, consent) to use this data in a commercial manner?
- Is the data of quality, and what commercial value does it have, and for whom?
- Who (third parties) would be interested in accessing and using this data? Would they want an exclusive license?
- Can you offer the data to a variety of entities on a nonexclusive basis?

Trademarks:

- Have you registered protection for your brand in relevant territories (for protected rights)?
- Are you going to use the brand exclusively yourself? Or are you interested in third parties using the brand for advertising your technologies, products and services?
- What types of use will you allow by third parties (licensees), and how are you going to verify this use is in accordance with your brand guidelines?

3.6. Channels to commercialization

IP assignment and licensing have been briefly discussed as the key income-generating activities. While these activities are considered in more detail in chapter 7, particularly in regard to mobile apps as a whole, the four main models for commercializing IP are as follows:

1. **Commercialization by IP owner**: this is the direct exploitation of the mobile app (and the IP in the mobile app) to customers, whether consumers or professionals.

Commercializing includes manufacturing fees, marketing and selling subscriptions or copies of the mobile app that embeds the technology to end customers.

2. **Assignment**: in this scenario, the app developer assigns the rights in the IP asset to a new owner; for example, an agency assigning all rights in a mobile app to its client (the app owner), or creatives assigning rights in customized or bespoke content to the app owner.
3. **Licensing**: the classic scenario, in which mobile app technology or the mobile app as a whole is licensed (for example, white branded) to a third party that wishes to use or commercialize the mobile app for itself as app owner in exchange for royalties or licensing fees.
4. **Joint ventures or partnerships**: in this scenario, the app developer or owner will partner with (usually) a larger company or investor to enable it to bring the technology to the market and find clients. The results are often jointly owned (or owned by a joint venture vehicle) and the income from commercialization is split.

An example of commercializing IP: visual recognition technology

Company A has developed visual recognition software (algorithms, training of machine-learning models and their implementation), including image capture and transmission for mobile devices and an online platform for image processing, recognition and integration with third-party services. This can be exploited via several different channels:

1. Direct licensing of visual recognition technologies in custom-built mobile apps for clients. The SDK for the mobile devices or mobile apps is often licensed for free to end customers, and income is derived from licensing the image processing technologies in the back-end server (engine for image recognition) provided as software as a service.
2. Licensing of mobile app SDK and back-end to clients, who license the mobile app technology as a SDK and also take a license to the back-end 'engine' for

in-house image processing and integration with product catalogues and sales platforms.

3. Joint venture for implementing the image recognition technologies in a particular sector, whereby Company A brings the recognition engine, the partner brings images or knowledge of the sector (apparel, machine parts) and they jointly build and commercialize customized mobile apps for companies in that sector (clothes, engineering and machinery).

The relationships, legal context and terms of the agreements that implement these business models and income streams is explored in chapter 5.

A case study: Music4you, IP based app revenue in the music sector

Given the success of Spotify, an entrepreneur in South Africa has spotted the opportunity for using freely licensed music (one of the popular Creative Commons licenses, available, for example, at the Free Music Archive) to provide a music streaming app. With Music4you the app owner uses public domain and permissively licensed music (CC BY, for example, the most permissive license) to promote music to gain audience, and then enters into licensing agreements with other authors and performers who have reserved commercialization rights (CC-NC license, for example). The mobile app provides the now common features such as playlists, music recognition, affinities, sharing and advertising (and removing advertising).

The mobile app is first launched for free (freemium model) and subsequent revenue comes from different streams:

- Paid-up subscriptions for advanced features for managing music and streaming, or for cancelling out advertising.
- Paid access to royalty-bearing music tracks, a percentage of which is paid upstream to the authors and performers through platforms such as Jamendo.
- Additional licensing fees for commercial exploitation rights (rights to communicate the music in a commercial setting, such as background music, gyms or restaurants
- One-off payments for specific uses of music tracks such as synchronizing.
- Providing access to locally produced works, not necessarily under open licenses, but promoting local bands, musicians and culture (again, freemium model for generating IP income for these bands and musicians).

Key issues for the entrepreneur are:

- Understanding the IP protection and licensing rights for audio works and the concept of open-content licensing (for more information on open-content licensing, including Creative Commons licenses, see chapter 9).
- Providing and monetizing value-added services over music that is actually available to all for free.
- Competitive positioning of the mobile app in a market where large content platforms offer their own services, and leveraging knowledge of and access to audio works under open licenses.
- Developing a relationship with local artists and negotiating royalty agreements with them or their agents.
- Technology for content delivery and streaming for mobile devices, and finding economic means for streaming large quantities of audio files.
- Privacy and profiling of user tastes, for affinities and developing a catalog of available music.

3.7. Other income streams

Licensing or assignment of IP is not the only income stream for apps and other players in the app space. As indicated, there are a significant number of business models in the sector, each based on one or other aspect of the app model. While the previous section looked at those income streams based on IP, this section presents other common models where income can be generated.

A brief summary of this complex economic environment is provided in Table 3.2 below.

Table 3.2 A summary of income streams in the app sector

Income stream	Description	Popularity (share)	Relevant trend/products
Advertising	Providing adverts directly, or space for third-party adverts provided by ad networks.	67 per cent of app revenue	AdMob, AdColony, AppLovin
Pay to remove advertising	Offering premium subscription to remove ads from the content being accessed, e.g., YouTube, YouTube Music.	Increasingly popular	Duolingo, HBO Max, Tinder

Pay for premium	Offering premium services or content for a monthly subscription (over freemium); e.g. Spotify.	Increasingly popular	
Hypercasual and similar advertising	Advertising in hyper-casual games; e.g., simple videogames, word games, and puzzles.	High volume but sensitive to market share	Flappy Bird, Going-Balls, Magic Tiles 4, Word with Friends, Candy Crush
In-app purchases	Purchase of different digital goods and services advertised in the app (e.g., games), including automatic subscriptions. Can be for this app or other services. Subscriptions accounted for some 70% of in-app purchase revenue for non-games.	Very popular	Most product and service apps, games, e-readers
Free trial to paid app (freemium)	A significant positive relationship between app trialability and purchasing intentions has been found. Many studies have demonstrated the impact of trialability on behavioral intentions to adopt mobile apps.	High	Content apps such as Spotify, online newspapers and videogames
Electronic word-of-mouth (eWOM)	Better placing in rankings, through reviews, ratings and recommendations.	Increasing	

Source: the authors. Includes data data.ai. “State of App Revenue 2023.” *data.ai*. publishing date month day, year; and <www.data.ai/en/go/total-app-revenue-insights-report-2023/>l; Adwan, A. S., and G. Sammour. “What makes consumers purchase mobile apps: Evidence from Jordan.” *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 16, issue 3 (2020): pp. 562–583.

This section also briefly considers revenue streams for other actors in the mobile app ecosystem, the third parties that are fundamental to the operation of mobile apps and provision of mobile app-based services:

- **App stores**: have by far the greatest influence and impact and usually earn fees through commissions on mobile app sales and in-app sales.
- **Platform providers**: technology platforms that operate and provide infrastructure services to the app owner (often for the mobile app back-end on the server) earn income from providing the infrastructure services (IaaS, SaaS, PaaS) and added-value services such as security, traceability, billing and accounting.

- **Service providers:** include digital wallets, payment gateways, and logistics and security services. These are essential for the mobile app industry as they provide the supporting financial and logistical services for ecommerce.
- **Advertising networks**: the intermediary between advertisers and the spaces where adverts are placed, centralizing ad content and content provision, and providing added-value services such as targeting and analytics. Income is usually derived from commissions on ads and clicks and sales promoted by the ads served by the networks.
- **Mobile network operators**: supply and run the communications networks to support mobile apps and the back-end services. Importance depends on territory. In Europe and the United States of America, there is much competition and they are limited to providing access to the Internet and data carriers (charging users for connection fees, through flat or variable fee or broadband). In other countries, their key role is as gatekeepers for mobile apps on the network and they may charge mobile apps for transactions carried by the network.

3.8. Conclusions

As stated in a 2021 WIPO tool on funding:

> "The mobile app ecosystem is comprised of various players that interact to make the app industry function. There are also various business models that app developers can choose to pursue once a product is launched."[4]

The different types of intangible assets, and the IP rights that protect them, are essential for many income streams, principally through licensing or assignment. IP protection

[4] World Intellectual Property Organization. *WIPO Tool on the Financing of Intellectual Property-based Mobile Apps*. WIPO, 2021. <www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo-tool-financing-mobile-apps.pdf>.

against unauthorized use enables the app owner and other IP-based businesses (content providers, among others) to take advantage of their exclusive rights to monetize their assets through a variety of income-generating activities.

A short case study in the videogames industry illustrates the income streams for apps, particularly gaming apps, which we have seen generate more than 50 per cent of the income in the app sector.

Examples of revenue streams for mobile videogames

There are a variety of ways in which a mobile videogame can be commercialized, some direct, and others indirect. Successful titles have managed to generate revenue as follows:

- Free-to-play is a common commercial model in mobile videogames, whereby the entire game is available for any user to play, but the user is able to optimize or improve their experience through in-app purchase**s**. These could include premium characters or items, cosmetic upgrades or in-game currency that helps with progression. Premium items may often be 'won' through buying loot boxes or *gacha*, though this practice is regulated in some jurisdictions. Genshin Impact is a popular game that uses this means of commercialization. Separate yet related to the above is where users pay a monthly fee to access premium content within the free-to-play game, such as with Roblox. In addition, free-to-play games will generate revenue through advertising, which can sometimes be switched off, for a one-off or recurring fee.
- Paying a subscription to access a library of games has become increasingly popular. For example, Netflix allows subscribers to download and play games on a smartphone or tablet provided that such games are verified through their platform. Apple provides a similar service through its Apple Arcade. Generally, publishers or developers will negotiate to become part of such a games library, and will be paid a fixed rate for the inclusion of an existing title or development of an exclusive title.
- Some premium titles have to be purchased upfront, although this is becoming increasingly rare in the mobile market. An alternative is where limited content (such as the opening chapter or levels) is provided free, with the option of purchasing the remainder. An example of this would be Super Mario Run, Nintendo's first foray into mobile gaming.

Further, should the characters in a game become popular, additional revenue can be generated through merchandising, which has been successfully done with games such as Fortnite and Angry Birds.

To determine which revenue model is fit for purpose for a videogame, it is important to determine the target demographic, the costs involved in development and user acquisition, and whether platform fees are payable upfront.

Some mobile app-related technology, or content providers, will be satisfied to sell their services or IP results to clients for one-off fees, obtaining ongoing or recurring revenue through repeat engagements or a variety of sources.

IP relevance cannot be overlooked. For example, income can be secured through a continuous stream of licenses that provide the app owner with royalties. Other monetization strategies involving IP include an outright sale of the IP (assignment), creating partnerships or joint ventures, or commercialization of the IP by the app owner on their own. Each model depends on the needs and resources of the app owner. What is clear is that most mobile apps have some IP attached to them and at the early stages of development this can prove to be a valuable intangible asset, especially when it comes to fundraising from investors.

Income Streams: Key takeaways

- There are many revenue streams available in the mobile app sector, for the different market actors.
- The market is set to grow significantly over the next five years.
- IP based revenue streams include:
    - straightforward licensing of IP rights such as patents or trademarks to use in mobile app solutions;
    - licensing or assigning mobile app technologies (mainly copyright licensing);
    - licensing content (audiovisual, designs, among others); and
    - data-related revenue (access and reuse of protected data)
- Non-IP based revenue streams include:

- advertising;
- premium services; and
- commissions on in-app purchases.

- Mixed revenue models include:
  - platform or infrastructure service subscription revenue (mix of service revenue and technology licensing).
- There are a number of channels to achieve income, including:
  - direct licensing to clients;
  - indirect licensing through OEM or third-party integrators; and
  - joint ventures and partnerships with third parties.
- App developers and owners should study the different revenue options, protect key IP assets that may be monetized through licensing or assignment, and obtain appropriate licenses for third-party technology, service or content providers, with revenue share or royalty-based streams.

3.9. Useful links and resources

Web references:

- Admiral Media: *An In-depth Guide To Freemium Mobile Apps*. Admiral.media. Visited March 2024. <www.admiral.media/an-in-depth-guide-to-freemium-mobile-apps/>.
- ADJUST: *How to make a freemium app: key benefits and best practices*. 2020. <www.adjust.com/blog/how-to-make-a-freemium-app/>.
- Data.ai: *State of App Revenue 2023*. <www.data.ai/en/go/total-app-revenue-insights-report-2023/>.
- FasterCapital: *Revenue Models for Mobile Apps*. Fastercapital.com 2024 www.fastercapital.com/content/Revenue-Models-for-Mobile-Apps.html.
- MobileAction: 8 proven App Revenue Models for your mobile app. Mobileaction.com. 2024 <www.mobileaction.co/blog/app-business/app-revenue-models/>.

Chapter 4. Legal framework and IP protection

4.1. Introduction to intellectual property rights in mobile apps

In our increasingly interconnected and innovation-driven world, IP rights have emerged as a critical framework for safeguarding creativity, innovation and the products of human intellect, and as a way to monetize it. This chapter outlines the various rights and their impact on mobile apps.

Before focusing on the IP relevant to the sector, it is worth mentioning its origins and purpose. The roots can be traced back to ancient civilizations that recognized the value of protecting creative works and innovations. However, it was not until the industrial revolution that IP laws began to take shape. The notion that creators should enjoy exclusive rights to their creations was formalized to encourage individuals and organizations to invest time, resources and ingenuity in new ideas, inventions and artistic expression.

In fact, historically, IP protection serves a dual purpose: to reward creators for their contributions and to promote the dissemination of knowledge. By granting creators exclusive rights to their works for a limited period, IP laws provide an incentive for innovation. This protection fosters an environment where creators are motivated to share their knowledge with the public, thereby enriching society as a whole.

A spectrum of IP rights exists, tailored to protect specific types of creations. This chapter will focus on those that are relevant to mobile apps such as copyright, patents, trademarks, trade secrets, designs and databases' sui generis rights.

While IP is often governed by domestic laws, organizations such as WIPO and international agreements including the WIPO Copyright Treaty (WCT) of 1996 play a pivotal role in harmonizing these rights across borders.

In the era of smartphones and apps, IP has assumed a central role in the development and deployment of mobile applications. More information is available from the WIPO

Intellectual Property Rights for Mobile Applications online toolbox, which includes the following:

- WIPO: *Protecting your Mobile App: Intellectual Property Solutions*. http://www.wipo.int/publications/en/details.jsp?id=4569
- WIPO: Intellectual Property and Mobile Applications https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1071.pdf
- WIPO: *Intellectual Property Toolbox for Mobile Applications Developers*. http://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo_ip_toolbox_mobile_apps.pdf
- WIPO: *The Role of Intellectual Property Rights in the Development and Commercialization of Mobile Applications*. https://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo_iprs_mobile_apps.pdf

4.2. Copyright

4.2.1. Copyright legal framework

Copyrights protect creations in the literary, scientific and artistic domain, whatever the mode or form of expression, provided they are original creations of the author. Besides literary, musical and artistic works, among others, copyright also protects computer programs.

The author of a copyrighted work is the individual (or group of individuals) who creates the work. The author is automatically granted the exploitation and moral rights indicated below from the moment of creation.

The copyright rights owner or rights holder is the entity that legally owns the copyrights to a work and may or may not be the same as the author. The rights holder and the author are not the same when the rights over the work are assigned from the author to the rights holder, either through a contractual or a legal assignment (for instance, the automatic assignment of right by employees to the benefit of the employer).

Co-authorship

The author (and/or rights holder) can be an individual/legal person or people. When multiple persons or entities collaborate, such as in the design and development of a mobile app and its backend on the server, they may all be coauthors and share a percentage of ownership of the rights, which is determined by the parties themselves.

The owner of copyright on a protected work has certain exclusive rights categorized as exploitation rights (or economic rights) and moral rights.

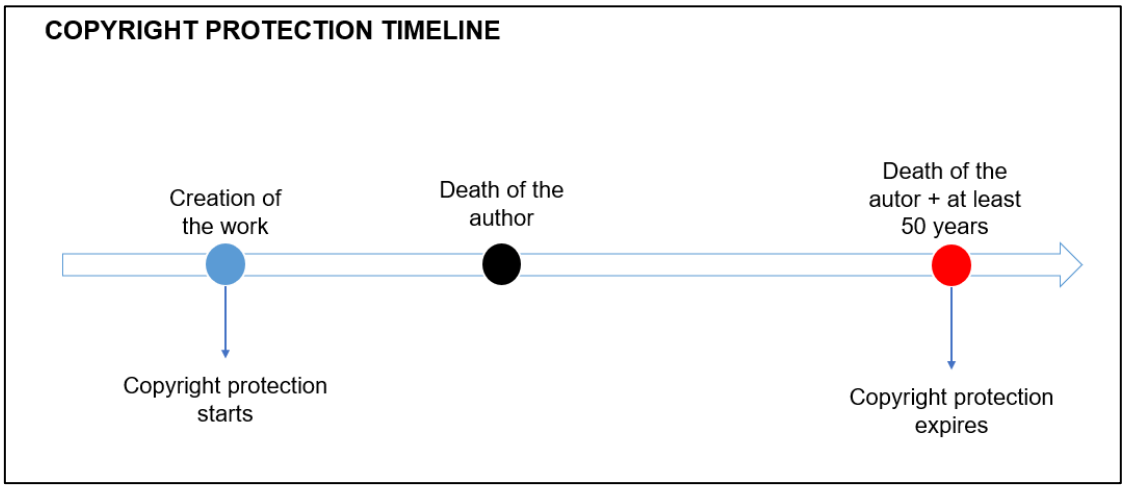
- Exploitation rights include the right to reproduce the work, and distribute, communicate to the public and transform it.
- Moral rights are the inalienable and nonwaivable rights belonging to the author, including the right to decide whether the work should be disclosed and in what form, and whether such disclosure should be made under their name or pseudonym, or anonymously, to demand recognition as author of the work, to modify the work complying with the rights granted to third parties over the work, and to withdraw the work from commerce.

In certain circumstances, the economic rights of the author or copyright holder can be limited, meaning that the protected work can be used without their authorization or payment of compensation. Those exceptions and limitations are country specific, but some are shared, such as the exceptions for educational and research activities, and for museums and libraries.[5] In other countries, such as the United States of America, an exception called fair use doctrine exists. This permits certain uses of copyrighted material, including criticism, commentary, news reporting, education and transformative purposes such as parody or satire. It is worth noting that courts evaluate whether certain uses qualify as fair use.

[5] More information is available on the WIPO website, www.wipo.int/meetings/en/details.jsp?meeting_id=53646.

Unlike other IP rights, such as patents or trademarks, copyright protection is granted from the moment of the work's creation, without the need for registration. The duration of copyright protection varies nationally, but generally, once granted, lasts for the life of the author plus at least 50 years, as set by the WIPO Copyright Treaty. In countries such as France, Italy, Spain and the United States of America, the duration is the author's life plus 70 years, in Kenya, and in Philippines and China, the author's life plus 50 years.

Figure 4.1 Copyright protection timeline



Source: the Authors.

Even though it is not required to obtain copyright protection, registering the work with IP registries (either traditional or blockchain-based) provides a public record and can be useful in establishing evidence of ownership in commercial transactions (such as financing) and legal proceedings (for example, the enforcement of rights).

Registration of copyrights

Formal registration can be useful, or even explicitly requested in certain circumstances. For instance, if you are looking for an investment, investors may ask you to present evidence of copyright ownership.

Given copyright grants rights to the author over the work, third parties are not allowed to use it without consent from the author (or the copyright holder). Third parties wishing to

use a copyrighted work need to enter into a license agreement with the author or the copyrights holder. A license is a legal agreement that grants permission to another entity (whether a legal person or an individual) to use the copyrighted work in specific ways outlined in the license itself, while the author or the copyright holder retains the copyrights on the work.

Unlike the license, a copyright assignment implies the complete transfer of ownership of the exploitation rights on a work to another party. Through the assignment of rights, the copyright holder no longer possesses the rights and control over the work, while the assignee becomes the new owner of the copyright over the work.

More information on the copyright legal framework is available on the WIPO website, www.wipo.int/copyright/en/.

Checklist for copyright protection

- Identify the different works involved such as computer programs, images or documents.
- Determine if the works can be protected by copyright:
  - Is it a production in the literary, scientific and artistic domain?
  - Is it original?
- Clarify who is the author/authors and if they are the same as the rights owner:
  - Who generated the work?
  - Was the work generated in the course of an employment relationship?
  - Does a contractual assignment exist (for instance, a case of a work for hire)?
  - Does the work include third-party copyright components and works, such as software libraries or audiovisual works?
- Consider registering the work to have evidence of the rights and their ownership:
  - Look for convenient registries.
  - Look for professional advice on registration.
- Check licenses over third-party components (for example, open-source components) and the permissions granted:

- Are the permissions sufficient for the purpose and/or does the license impose limitations?

- Does another entity want to use the protected work, or are app-related technology or other works being developed for a client:
  - Consider whether you want to license or are required by the client to assign the works to them?
  - Consider the variables of the license/assignment (duration of the license, fees to pay, authorized uses, limitations).
  - Look for professional advice for drafting a license/assignment.

4.2.2. Mobile app elements protected by copyright

a) Code

The fundamental component of all software is computer code, and mobile apps are no exception. Copyright law protects source code and object code (or binary code) with equal measure. This means that authors, or right holders, of software code either in object or source form have the exclusive rights to use the code, copy it, modify it and provide copies to other people, among other things.[6]

The implications of software copyright protection include:

1. Other entities cannot use your code without your permission; that is, a license.
2. You cannot use software code written by other persons or entities without their permission (a license), or without them assigning the rights over the code to you.

[6] World Intellectual Property Organization. *Protecting your Mobile App: Intellectual Property Solutions*. WIPO, 2021: part II, sect. B.1.

Example software license

You may find an open-source license included in the license section of an online repository such as GitHub or GitLab, such as the following license known as the “MIT license”:

> *Copyright (c) 2023 John Developer*
>
> *Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the ‘Software’), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:*
>
> *The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.*
>
> *The software is provided ‘as is’, without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the software or the use or other dealings in the software.*

Or you can find sentences similar to the following in a website’s terms and conditions:

> *Prohibition to use the code for commercial/business purposes: “The content of this website, including any image, text and software code, can be used for personal purposes only. All commercial or business purpose is strictly prohibited.”*

Some sites allow published code to be used for commercial purposes as well:

> *The content of this website, including any image, text and software code, can be used for any purposes, including commercial ones. You can copy, reproduce, distribute and make available to the public the content of this website, provided you mention the website owner as a source of the content.*

Tips on licensing software

Using and licensing software is not straightforward, and the following tips can be useful:

- **Granting a license**: when you allow someone to use your software, you will enter into a license. Different kinds of licenses exist (proprietary license, open-source license, source-available license, among others) depending on, for example, the activities you allow (or prohibit) the other entity to do, or if you look for compensation. Before negotiating a legal agreement, you should be clear what type of license to apply. For more information on open-source licenses, see chapter 9.
- **Using software code found on the Internet**: just because you find pieces of code on the Internet (for instance, on websites or software repositories like GitHub), it does not mean that no one owns rights over it. A license is always required to use software code. Study the repository license section, or the website's terms of use for legal wording allowing or limiting use of the code. If no permission is included, refrain from using it.

b) Graphical user interfaces

A graphical user interface (GUI) is a visual interface that allows users to interact with electronic devices, software or computer systems through graphical elements such as icons, buttons, menus and windows, as opposed to using text-based commands.

As with the protection of software code, copyright can protect GUI code as well. GUI peculiarity is often not in its code itself, rather in its appearance and the look and feel that its components generate. In essence, the appearance of a GUI can be eligible for copyright protection if it is original and not designed solely for its technical function. This protection would apply only to the aesthetic elements of GUIs, not to their functionality. Some legal systems extend copyright safeguards to GUIs that demonstrate originality and being 'non-commonplace', resulting from developers making design decisions not driven solely by functionality.

It can be difficult, though, to demonstrate that the design of as a GUI as a whole, as well as its elements, are original, given they are often based on generic designs of, for example, icons or graphics. In this regard, European and US courts have denied protection to GUI elements considered dictated by functional needs rather than by aesthetic ones. It is important to note, however, that copyright protection might not be granted to non-commonplace designs considered functional within the confines of the applicable legal framework (though they may have design-right protection).

Even when GUIs are protected by copyright, the protection might not be strong. In fact, a GUI could be protected against verbatim copies, while imitating more generally the 'look and feel' would not be considered an infringement, unless an exact copy is made.[7]

The implications of a GUI being protected by copyright include:

1. The copyright owner has the exclusive right to copy, modify and distribute a work, unless an exception applies. Other entities need a license to perform these activities on their GUI.
2. App developers need to exercise care and avoid copying third-party GUI elements such as images, icons or animations that display distinctive creativity without authorization (unless an exception applies).

Example of GUI protection: TikTok

The most downloaded mobile app worldwide in 2022 was TikTok.[8] Let us take TikTok as an example, and apply what we have learned in this section about copyright:

- TikTok's software code, both binary and source code, is protected by copyright. The right owner is TikTok Pte. Ltd.
- If an app developer wants to use some bits of TikTok's code, they need a license. TikTok makes some pieces of its code available to developers under

[7] World Intellectual Property Organization. *Protecting your Mobile App: Intellectual Property Solutions*. WIPO, 2021: part III, sect. B.1; and World Intellectual Property Organization. *Intellectual Property Toolbox for Mobile Applications Developers.* WIPO, 2021: sect. 4.1.1.2.
[8] Statista. "Leading mobile apps worldwide in 2022, by downloads." *statistic com.* Jan. 9, 2023. <https://www.statista.com/statistics/1285960/top-downloaded-mobile-apps-worldwide/>.

different licenses, for those developers to build TikTok sharing and authentication experiences within their mobile app. For example, the SDK for Android that features the TikTok Login Kit and Share Kit is provided to developers on TikTok's developers site.[a]

- One of the characteristics that has made TikTok successful is its GUI, which includes videos that automatically start playing when the app is opening, the swipe interaction model and videos in full-screen mode. TikTok is aware of this, and in its terms of service, reserves all rights on 'look and feel' as part of the TikTok Content.[b]

a. Overview to TikTok for Developer Documentation. Tiktoc.com. March 2024 <https://developers.tiktok.com/doc/overview/>

b. TikTok. "Terms of service (U.S.)." *tiktok.com*. Nov. 2023. <www.tiktok.com/legal/page/us/terms-of-service/en

4.3. Patents

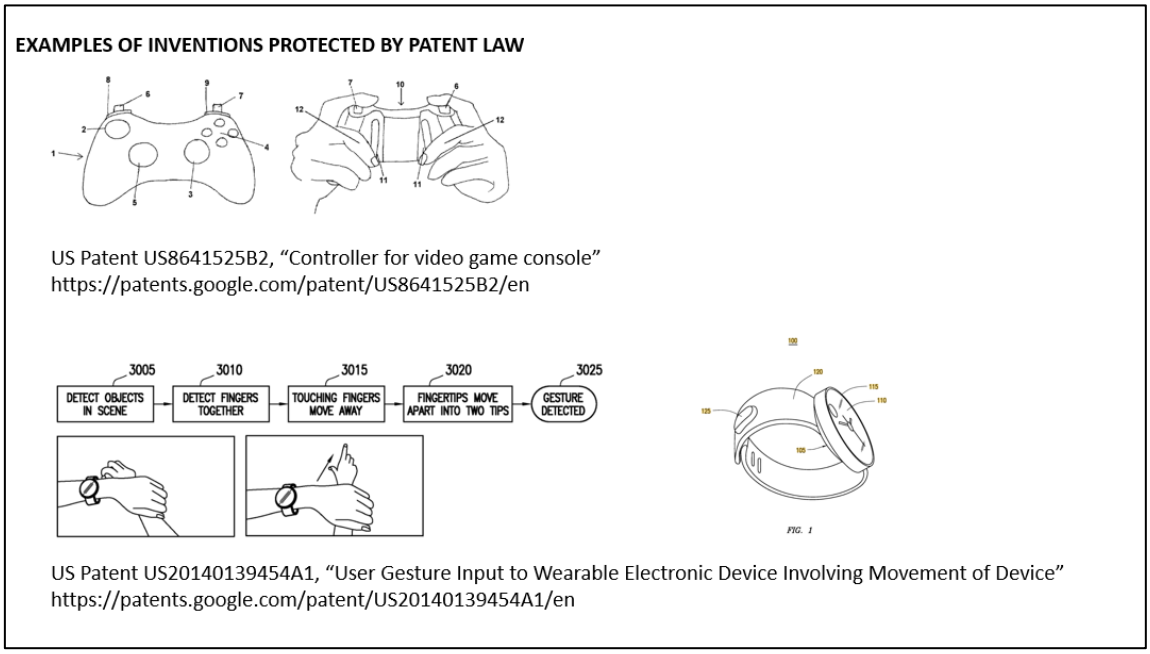
4.3.1. Patent protection legal framework

Patents protect technical inventions, and are often considered a "new solution to a technical problem". Inventions can be either products or processes. To be eligible for patent protection, an invention must:

- be new, meaning it is not known in the specific technical field,
- involve an inventive step, or be nonobvious for a person having ordinary skills in the relevant technical field, and
- be capable of industrial application.

In addition, the subject matter of the patent must be patentable under the relevant country law (some states prohibit patenting certain inventions such as mathematic methods, plant or animal varieties and commercial methods). Finally, a valid patent application must disclose the invention sufficiently clearly and completely to enable a person with ordinary level of skills to replicate it. For more information, read the WIPO booklet, What is IP?.

Figure 4.2: Examples of patentable inventions



Source: As indicated in the figure.

Patent tips

There are millions of patents around the world and new applications are filed daily. To ensure an invention can be patented, it is recommended a patent search is performed, with the support of a professional. The search assesses novelty and determines whether there are existing patents or publications that could impact the ability to obtain a patent for that invention.

To ensure an invention is new, every person accessing the invention and the relating documentation should be bound by confidentiality obligations. If it is disclosed before the patent application, it will not be possible to patent the invention

The inventor of a patent is the individual, or individuals, who contributed to its creation. The inventor is granted the patent rights identified below from the moment of the patent grant.

The patent rights holder is the entity (individual or company) that legally owns the patent rights to an invention, and may be the same as the inventor. In particular, and similar to copyright, the inventor and the rights holder are not the same when the former assigns

the rights to the latter through a contractual agreement or legal assignment. In certain circumstances, the rights on the invention do not belong to the inventor but are legally assigned to a third party such as an employer. These circumstances depend on domestic law but, in general, inventions generated by employees belong to the employer, as do inventions generated by researchers working in public universities and other research institutions.

The owner of the patent rights is granted the right to prevent third parties that do not have their consent from: (1) manufacturing, offering for sale, introducing into commerce or using the patent, (2) using a process that is the subject of the patent, or offering such use, when the third party knows or circumstances make it evident, that the use of the process is prohibited without the consent of the patent holder, and (3) offering for sale, introducing into commerce, or using a product directly obtained by the process that is the subject of the patent, or importing or possessing that product for any of these purposes. It is important to note that the rights granted are limited to the territory where the patent is granted.

Patents grant exclusive rights to the inventor or right holder, though these can be affected by certain exceptions and limitations. Exceptions are mainly aimed at enhancing public welfare, public health and research, and in circumstances where exclusive rights on specific inventions would not enhance such welfare. While territory specific, there are some exceptions that are generally implemented, such as that for private or noncommercial use, experimental use and/or scientific research, extemporaneous preparation of medicines, compulsory licenses and/or government use.[9]

Patent rights are not generated automatically on creation of the invention but are consequent on registration. This means that once an invention is created, if the inventor

[9] More information on patent limitations and exceptions implemented worldwide is available on the WIPO website, www.wipo.int/meetings/en/details.jsp?meeting_id=30925 and www.wipo.int/meetings/en/details.jsp?meeting_id=32102.

considers that it meets all the requirements of a patent, they have to file a patent application with the patent office where they want the patent granted.

As previously mentioned, patent rights are territorial, meaning that they exist in the territory where the patent is granted. For this reason, inventors should seek protection in the territory where they operate, or where they want to prevent their competitors from using the patented invention. Each country has its own patent office, and regional patent organizations also exist to help obtain protection in more than one country at a time. Examples can be found at WIPO's Directory of Intellectual Property Offices.

Once the patent application is filed, it goes through the grant procedure. Here, the application and invention are analyzed to ensure all formal requirements are included and that the invention meets all the requirements to be patented. The process is lengthy and costly: the grant procedure takes from two to five years, with the fees specific to the country/region, process selected and type of patent. Inventors are encouraged to consult the websites of relevant patent offices for updated information on fees. Every patent office has its own specific time line; nonetheless, below you can find a general simplified time line of patent protection, taking into account a general national patent office.

Once the patent is granted, the rights are generated. Their duration is limited to 20 years. It is important to note that once the patent is granted, it is protected from the time of the patent application filing date, meaning that the rights are enforceable against third parties using the patent without the inventor or right holder's consent from the patent filing date.

When an invention is patented, the patented product or method cannot be used or implemented by persons other than the inventor (or the right holder) without their consent. This consent comes in the form of a patent license, a legal agreement where the patent right holder specifies the use the licensee can make of the patented invention, usually in exchange for fees. The ownership of the rights stays with the inventor/right holder, but the third party can use the invention, and manufacture and sell products embodying it.

Patent rights can also be assigned by the inventor or right holder to another entity. A patent assignment implies the complete transfer of rights to another entity, so that the original inventor or right holder no longer possesses those rights.

More information is available on the WIPO website, www.wipo.int/patents/en/ and www.wipo.int/edocs/pubdocs/en/wipo_pub_450_2020.pdf.

A checklist on patent protection

- Identify any new and inventive technical solutions created for the mobile app.
- Determine whether the invention can be patented and the type of patent:
  - Is it a 'new solution to a technical problem'?
  - Does it meet all requirements (novelty, inventive step, industrial application, not an excluded invention, able to be disclosed in a clear and complete way)?
  - Is it a product or a process?
- Determine who is the inventor:
  - Who created the invention?
  - Does a legal or contractual assignment exist?
- Document the invention:
  - Maintain records, drawings, descriptions and results related to the invention to prove originality and novelty.
- Determine in what countries you want your invention to be protected:
  - Where do you want to commercialize it/a technology based on it?
  - Where you want to prevent your competitors from using it?
- Seek professional advice for a patent search and preparing the application.
- Does another entity want to use your patented invention:
  - Consider the variables for a license (duration, fees, allowances, limitations, territory, among others).
  - Look for professional advice for drafting the license.

4.3.2. Mobile app elements that could be protected by patents

a) GUI (functional elements)

Different aspects of GUI can be protected by different IP rights. We have seen that copyright can under certain circumstances protect the aesthetic aspects of GUI, beside its code. GUI functional aspects, on the other hand, may qualify for protection under patent law, though currently, under both the European and the US patent systems, obtaining such protection is rare.

In the United States of America, the applicant would have to show that the patent improves the functioning of the computer itself or an existing technological process, and for GUIs this was not the case. In the European Union, inventions excluded from patents include the presentation of information and programs for computers. In order to be patentable, GUIs must have a technical character consisting of an improvement to the internal working of a device, or a physiological impact on how the mobile app user interacts with the app.[10]

Given the different approaches across jurisdictions, seeking local advice is recommended.

b) Mobile app functionalities

Patent law can be a viable option for protecting specific ways of implementing a mobile app feature (but not a feature itself); for example, functions for security and authentication, data processing, encryption or mobile transmissions. Features that are hardware implemented inventions, especially data transmission protocols, may obtain patent protection, but such protection is more difficult to obtain for software implemented functionalities, which are in the majority in the mobile app space.

---

[10] World Intellectual Property Organization. *Protecting your Mobile App: Intellectual Property Solutions*. WIPO, 2021: part III, sect. B.4 and 3.4.4; and World Intellectual Property Organization. *Intellectual Property Toolbox for Mobile Applications Developers*. WIPO, 2021: sect. 4.2.2.2.

Vis à vis the protection process, in certain jurisdictions it is mandatory to describe the code or algorithm underlying and allowing the execution of a feature, but not in others. In such cases, it is necessary to disclose the steps for implementing the specific features. As a consequence, competitors may be able to implement similar functionalities without infringing rights, following a different process or using different algorithms or code.[11]

c) Code

Patent is not the best option for protecting software code for two reasons. First, the length of the patent grant process (approximately two to five years, depending on the patent office involved) is incompatible with the ephemeral nature of software code, which is frequently amended and improved. And second, many countries explicitly exclude computer programs as such from patent protection.

In certain circumstances it might be possible to patent inventions implemented by software (and there are many examples), but the length of the process may mean relying on copyright and/or trade secrets is preferable.[12]

d) Software architecture

To obtain patent protection for any invention, it must meet all the requirements set out by patent law, including novelty. With regard to software architecture, this means it must be computationally more efficient than other similar applications in that, for instance, it requires less time and fewer internal resources.[13]

Case study: Amazon's one-click purchase patent

In 1999, Amazon was granted a patent on its famous one-click purchase feature (U.S. Patent No. 5,960,411). The invention is a method for single-action ordering of items in

[11] World Intellectual Property Organization. *Protecting your Mobile App: Intellectual Property Solutions*. WIPO, 2021: part IV, sect. C.
[12] World Intellectual Property Organization. *Protecting your Mobile App: Intellectual Property Solutions*. WIPO, 202: part II, sect. B.1; and World Intellectual Property Organization. *Intellectual Property Toolbox for Mobile Applications Developers*. WIPO, 2021: sect. 4.2.2.1.
[13] World Intellectual Property Organization. *Protecting your Mobile App: Intellectual Property Solutions*. WIPO, 2021: sect. 3.2.2.

a client/server environment. The novelty was in the reduced number of purchaser interactions necessary to place an order, as well as the reduced amount of information transmitted between the client system and server system. In 2007 the patent was significantly reduced, and it expired in 2017, with the system now implemented by several mobile apps and web platforms.

The grant of the patent was largely criticized and defined as a patent office gaffe.[a] In recent years, their approach has been more conservative, with offices limiting the granting of patents over functionalities such as Amazon's one-click purchase.

[a] "Patently Absurd." *Forbes Newsletters*. Forbes, May 29, 2000. <www.forbes.com/global/2000/0529/0311090a.html?sh=5d08bcd97158>.

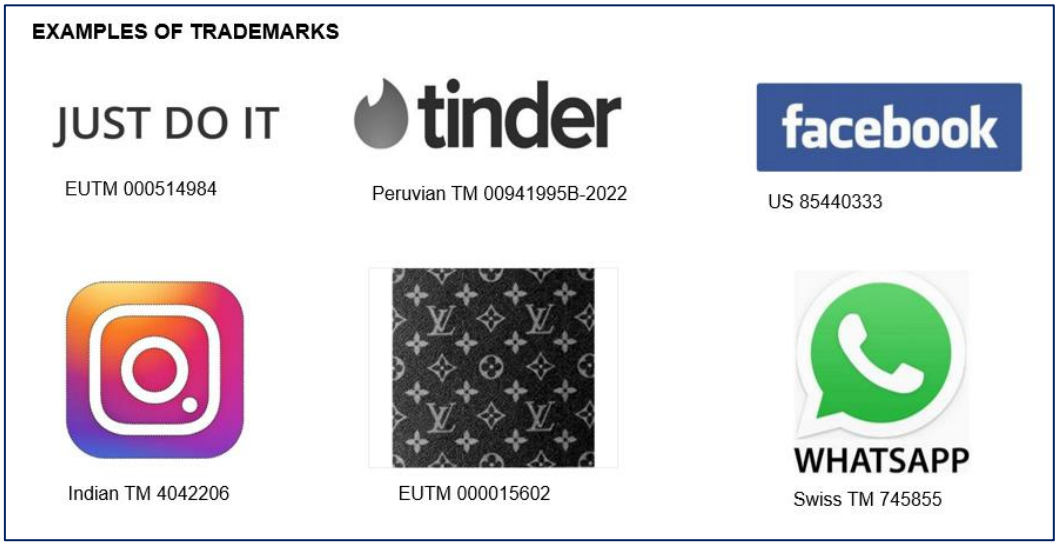
4.4. Trademarks

4.4.1. Trademark legal framework

A trademark is a right that protects a sign used in commerce. It may consist of words, images, designs, symbols, letters, numbers, colors, 3D features such as shape or packaging of goods, or even sounds, provided they are capable of distinguishing the goods or services of one enterprise from those of another one.

Depending on the country, some signs cannot be registered as trademark; for example, marks that are contrary to morality, or that have become customary in the current language or lack any distinctive character.

Figure 4.3 Well-known and famous trademarks



Source: websites of companies represented by the indicated trademark.

The trademark owner is the individual or entity that applies for registering a trademark. More than one owner may hold joint rights in the registered trademark.

Registration of a trademark gives its owner or rightsholder the exclusive right to use the mark in commerce in the territory and for the products or services for which the mark is registered. In particular, the owner is entitled to prevent third parties that do not have their consent from using signs in the territory of registration that are identical or similar to the registered trademark, for product or services similar or identical to those for which the trademark is registered. Owners of trademarks that have a reputation in a territory may be granted additional protection in certain countries.

As with copyright and patents, the rights granted by trademarks are subject to certain limitations and exceptions. They are country/region specific; for example, the European Union sets out that trademark owners cannot prevent any third party from: (1) using their name or address in the course of trade, (2) using signs or indications that are not distinctive or concern the kind, quality, quantity, or other characteristics of good and services, and (3) using a trademark for identifying or referring to goods or services as those of the proprietor of that trademark.

Trademarks are protected from the moment of registration with a national or regional trademark office, though there are countries with unregistered trademark rights. Entities seeking to protect their trademarks have to file a trademark application to the office of the territory where they seek protection.

The length of the process and the fees for registering a trademark vary depending on the office, and it is advisable to check office websites for updated fees and statistics.[14]

Trademark Tips:

It is highly recommended seek help from professionals for checks of preexisting similar or identical trademarks to reduce the risk of opposition during the registration process.

Like copyrights and patents, entities that do not own a trademark require the owner's consent to use it. This consent takes the form of a license in which the owner specifies the activities that the licensee can undertake, along with any limitations. If a trademark owner wishes to transfer the ownership of the trademark, they must assign it to the new owner and update the information with the relevant trademark office.

More information on trademark protection is available on the WIPO website, www.wipo.int/trademarks/en/ and www.wipo.int/edocs/pubdocs/en/wipo_pub_450_2020.pdf.

Checklist for trademark protection

- Design the mark or sign you wish to use to identify the company or app.
- In which territories will you use the trademark?
- Ensure your trademark meets all requirements to be registered in the territory:
  - Is it distinctive?

[14] For more information on the procedure for registration, See World Intellectual Property Organization. <*Intellectual Property Toolbox for Mobile Applications Developers*. WIPO, 2021: sect. 4.3.3.2.>

- Does it fall under one of the symbols that cannot be registered in the territory?
- Check additional territorial requirements.

- Enlist professional advice to determine the product and services classes you want your trademark to be registered for, and to ensure no similar or identical trademarks exist in the territory for similar or identical products/services.
- File the trademark application and pay the relevant fees.
- Ensure you pay the renewal fees and file any additional documentation for renewing the trademark.
  - Are you interested in maintaining the trademark? If not, you do not need to renew it.

4.4.2. Mobile app elements protected by trademark rights

a) The mobile app's logo or name

Trademarks serve as identifiers distinguishing a company's products or services from those offered by other companies in the market. In the mobile app environment, trademarks have great value, given users recognize specific mobile apps from their name and/or logo amid the plethora of mobile applications published in app stores. Think of the WhatsApp green logo, Twitter's blue bird (in 2023 substituted with an X), TikTok's white note on a black background, among others – you know these mobile apps by glancing at their logos without ever reading the name.

In the mobile app intangible and dynamic market, it is important to be recognized by users, who are an app's customers. Applying for a trademark is a smart and relatively cheap move, as the protection is granted for 10 years and prevents competitors from using an identical or similar mark for their mobile app.

When deciding your mobile app's name or logo, ensure it helps distinguish your mobile app from others in the market. Avoid marks or logos similar to ones that already exist, or that could confuse users and result in an infringement of another company's trademark.

b) Color combinations used in mobile app

Beside the mobile app's name and logo, there are other elements that can be protected as trademarks. One such element is the color, or color combinations, used in the app, in particular when they are distinctive. This means the color(s) can be registered if customers identify the mobile app by the color only. It is important to state that when registered as trademarks, the color must be identified with the color code. For color combinations, the sample and description of how colors are arranged are also necessary.[15]

c) Aesthetic elements of GUI

Another aspect of apps that can potentially be protected by trademark (or literally, as a trademark) is its GUI. For GUIs (or their components) to be registered, they must be capable of helping the public to identify the origin of a product or service, without reference to other signs such as a logo or brand name (provided that the logo or brand name are not included in the user interface). This is particularly difficult to prove prior to the app's launch.

It is important to bear in mind that only aesthetic elements of GUIs can be registered as trademark, given that functional or technical elements are excluded from this type of protection. Thus, all the parts of a user interface that perform a function of the mobile app cannot be registered. With aesthetic elements, we refer to the icons used in the interface, its layout and icon positioning, and dynamic elements, among other things. Before applying for protection for such items, seeking local advice is recommended, as it may not be registrable in certain countries. In addition, the elements of user interfaces can be registered individually or as a whole. Countries such as India allow GUIs to be

[15] World Intellectual Property Organization. *Intellectual Property Toolbox for Mobile Applications Developers*. WIPO, 2021: sect. 4.3.2.2.

registered as a whole, provided they comply with the requirements set out in the applicable laws.[16]

Further, it is important to bear in mind that, to be protected as trademarks, GUIs must not be similar or identical to earlier marks.

Case study: Instagram-related trademarks

The social network mobile app Instagram has been well known worldwide for a decade. Original owner Instagram LLC and current owner Meta Platform Inc. protect the mobile app name and logos by means of an extensive trademark portfolio.

As of August 2023, more than 400 trademarks (registered and applied for) relating to the Instagram name and logo existed in the international trademark database TMview,[17] owned by the company providing the mobile app. The trademarks are registered in 44 IP offices, both national and regional. The elements registered as trademarks are:

- The word INSTAGRAM.
- The word INSTAGRAM with the specific font used in the mobile app:

- The mobile app's logo.

The trademarks are registered for diverse products and services. In the European Union, the word INSTAGRAM (European Trademark 017739392) is registered for all 45 classes of products and services. Beside this exception, the most recurring classes of products and services to which the trademark relates are classes 9 (computer software), 35 (advertising), 41 (entertainment) and 42 (software-related services).

[16] World Intellectual Property Organization. Protecting your Mobile App: Intellectual Property Solutions. WIPO, 2021: part III, sect. 3; and World Intellectual Property Organization. The Role of Intellectual Property Rights in the Development and Commercialization of Mobile Applications. WIPO, 2021: sect. 3.4.2.

[17] More information is available on the European Union Intellectual Property Network (EUIPN) website, www.tmdn.org/tmview/welcome#/tmview.

Instagram's trademark portfolio protects the app's logo and name in an exhaustive way, globally. As one of the most famous mobile apps in the world, it is important to protect its value from companies that may use a similar or identical mark to take advantage of its fame.

For new and/or local apps, such extensive protection is not necessary and is extremely costly.

4.5. Trade secrets

4.5.1. Trade secrets legal framework

The definition of "trade secrets" entitled to legal protection varies depending on the country. In general, they are described as valuable business information that derives value from not being generally known and that is subject to reasonable efforts to maintain its secrecy.

The Coca Cola secret

A famous trade secret is the Coca-Cola formula, which has been kept under wraps for more than 100 years.

The owner of trade secret is the person or entity with control over the trade secret.

The owner of a trade secret is protected against acquisition, use or disclosure of such secrets by or from third parties without their consent. The specific protection depends on the country, and usually prohibits these practices as unfair competition or as a violation of trade secret rights.

Trade Secret Tips: measures to protect trade secrets

Companies should take preventive measures to protect trade secrets against theft or misappropriation, including:

- Using nondisclosure agreements (NDAs), where employees and business partners sign an NDA that prevents them from disclosing a company's confidential information.

- Using noncompete agreements (NCAs), where employers ask employees, contractors and consultants to sign a NCA to prevent them from entering into competition when their employment/service agreement ends.
- Robust IT security infrastructure and information security policy.
- Controlling the accessibility of important documents.
- Establishing and maintaining a trade secret policy.

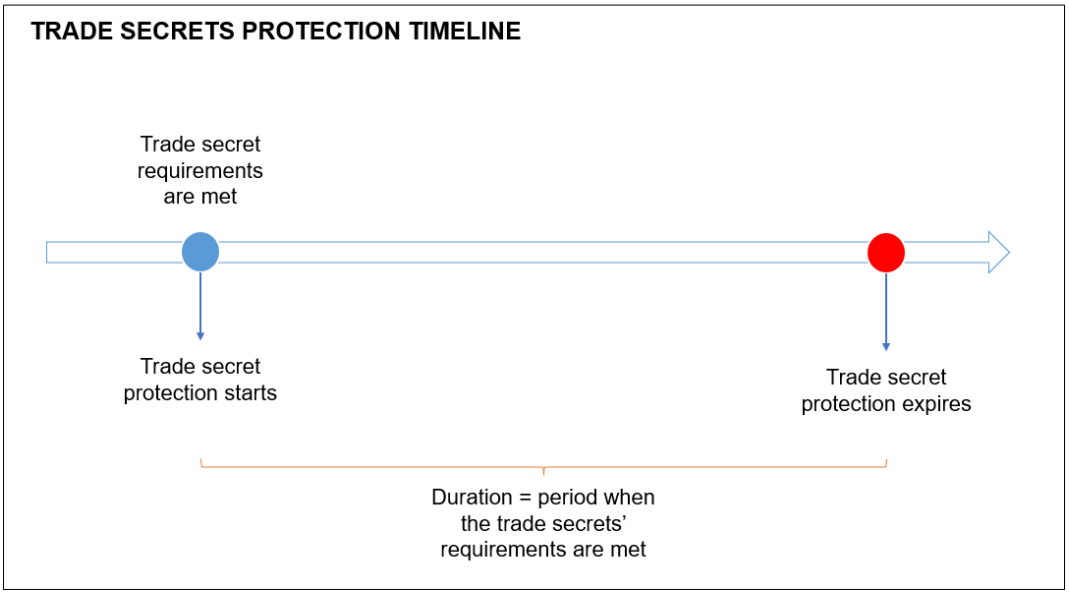
Source: World Intellectual Property Organization. “How to Protect Trade Secrets.” *wipo.int*. Web. Dec. 25, 2023. <www.wipo.int/tradesecrets/en/protection.html>; and World Intellectual Property Organization. *The Role of Intellectual Property Rights in the Development and Commercialization of Mobile Applications*. WIPO, 2021.

Even though trade secrets are generally protected against unauthorized access and use, in some circumstances such conduct is considered lawful even without the owner’s consent. Specific cases depend on the individual country, but they share some common principles. For example, trade secrets are considered lawfully acquired when this is done through legitimate means (that is, for example, no theft, bribery or misrepresentation is performed) and if the recipient has not violated any contractual or legal obligation related to maintaining secrecy.

Confidential information is protected as trade secret when all the requirements for being considered a trade secret are met. It is critical to have evidence that the information is a trade secret to enjoy the protection granted by the law. Further, trade secret protection lasts as long as the information meets the indicated requirements (see Figure 4.4). Therefore, as long as the piece of information is valuable, is not known and is protected by security measures to keep it secret, it is protected as a trade secret.

Trade secret protection is enjoyed only if the information is kept secret by its owner, meaning it is fundamental to protect the information with appropriate physical, logical and legal security measures and, from a contractual perspective, enter into confidentiality agreements with any third party having access to the information. For details on contractual measures, see chapter 5.

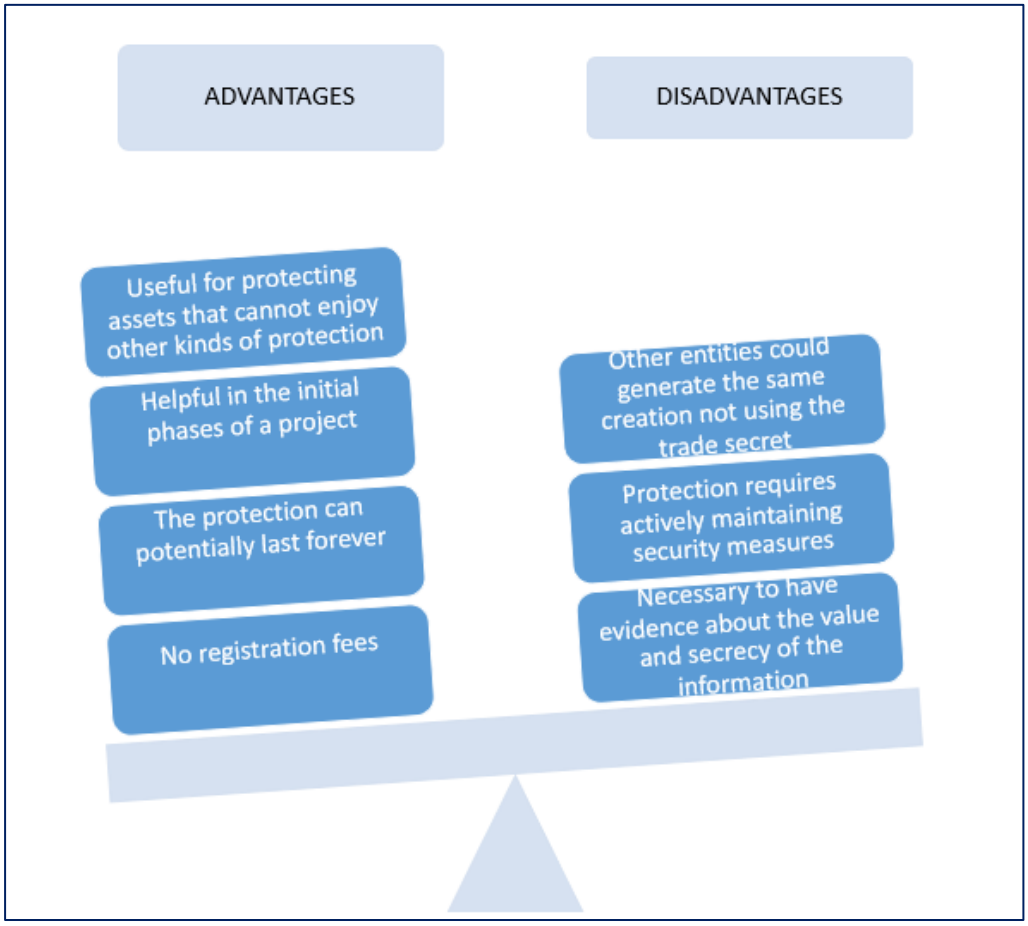
Figure 4.4 Trade secret time line



Source: Authors.

Trade secrets may need to be shared with someone for specific purposes. For example, an algorithm will be shared with employees or external consultants who need to work on it. Trade secrets may also need to be shared with collaborating companies. It is imperative that everyone, internal or external to the company, is bound by a confidentiality agreement before accessing the trade secrets and consents to comply. Overall, trade secrets present advantages and disadvantages, as summarized in figure 4.5.

Figure 4.5 Pros and cons of trade secret protection



Source: Authors.

More information on trade secret protection is available on the WIPO website,

www.wipo.int/tradesecrets/en/.

A checklist for trade secret protection

- Identify all materials, data and designs, among other things, and other information that is valuable for the company or venture.
- Ensure this information you want to protect qualifies as trade secret:
  - Is it not known by other market operators?
  - Is it valuable for your business? Is it valuable for being secret?
  - Are you implementing measures to keep it secret?
- Implement a trade secret policy covering storage, access and protection measures.
- Ensure all third parties with access to the information are bound by nondisclosure obligations.

- Periodically review your trade secret policy and all measures applied to keep the information secret:
  - Improve the policies and measures as necessary.

4.5.2. Mobile app elements protected by trade secrets

a) Code and architecture and data

Trade secret protection is particularly important in the initial phases of the conception, design and creation of a mobile app, when information is not yet made available to the public, but it is also important in the later stages of development.

Elements that can be considered and protected as trade secrets are the software code and architecture of the mobile app, when not made publicly available. This can be the case with cloud-based apps, or code that is not made available (for example, the code of new features or new apps).[18] Data collected, generated and used by the app also has commercial value and can be protected by trade secrets.

b) Functional aspects of GUIs

GUI and its elements can be treated and protected as trade secrets only prior to their launch with the mobile app, or with subsequent versions or updates.

The source code of GUIs can be protected as trade secret, as this is not usually distributed with the mobile app, though this might not be the best form of protection. Indeed, a developer could reproduce the same GUI functionalities without having access to the source code and, therefore, without infringing any trade secret right.[19]

[18] World Intellectual Property Organization. *Intellectual Property Toolbox for Mobile Applications Developers*. WIPO, 2021: sect. 4.5.
[19] Ibid.

c) Underlying idea, features and preliminary design documents

Trade secret protection can be used for protecting elements of the mobile app that either cannot be protected by other IP rights, or can be protected at a later phase.

Underlying ideas and preliminary documents such as drafts, meeting minutes and sensitive emails are likely to be one of the most relevant assets of a mobile app, and of any business, as well as its features before the mobile app is commercialized. For this reason, keeping them secret and protecting them in an appropriate manner is a good move, to ensure they are considered as trade secrets and protected.[20]

Therefore, especially in the prelaunch phase, it is essential to have a trade secret policy in place to reduce any third party gaining access to the product or services before launch.

Examples: Google and Uber's trade secrets

In the technology sector, there are some examples of technologies considered trade secrets (see below) but be mindful that their status may change with the passing of time: for instance, a company may decide (or be forced by law) to disclose their trade secrets, making these secrets public information.

- **Google Search algorithm**: Google has been keeping the algorithm behind our daily forays in its search engine secret for years. Its value is evident, and it is considered a trade secret, even though the company provides a high-level explanation on how the search engine works.
- **Uber surge pricing algorithm**: Uber, one of the first mobile apps for connecting car drivers with passengers, has its own algorithm for dynamic pricing and driver (or rider) matching. While the company gives information on the model on its website vis-à-vis the algorithm adjusting rates based on variables, including time and distance of the route, traffic and the current rider-to-driver demand, there are no details on how it works, or access to its source code. For this reason, it is likely to be considered a trade secret.

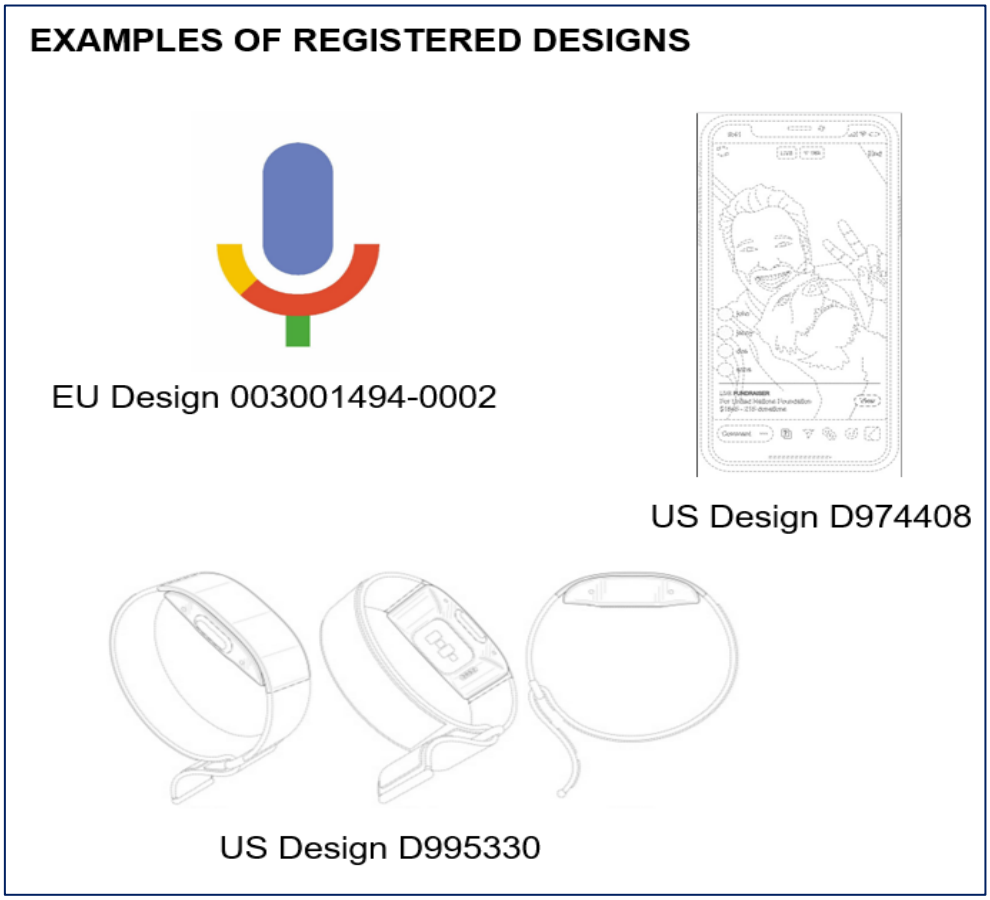
[20] World Intellectual Property Organization. The Role of Intellectual Property Rights in the Development and Commercialization of Mobile Applications. WIPO, 2021: sect. 2.2.

4.6. Design rights

4.6.1. Design rights legal framework

Design rights protect the appearance of the whole or a part of a product, including its shape, contours, color, texture, materials or ornamentation. In some countries, Japan for example, graphical elements such as icons may have design protection. To be eligible for protection, the design must be: (1) new, meaning that it must not be identical to existing designs, (2) distinguishable from other earlier designs, and (3) ornamental and not dictated by technical functions. It is important to note that in some countries certain designs might not be eligible for registration and thus protection. This is especially the case for designs that go against public policies or principles of morality.

Figure 4.6 Examples of registered designs



Source: Authors collected from EU and US design office database.

The owner of the design rights is the designer, or, if more than one person contributed, the designers. In certain circumstances, such as employment relationships, the design rights are legally assigned to other entities, similar to copyright and patents.

Design rights are not generated automatically on the creation of the design. Rather, they require registration. The registration of a design gives the owner exclusive rights to it, in the territory of registration. In particular, the owner of a design has the right to prevent others from making, selling or importing products bearing a design that is a copy or a substantial copy of their design, if these acts are performed for commercial purposes.

Like other forms of IP rights, design rights are subject to limitations in specific situations, to strike a balance with competing interests, including the public interest and competition. These limitations can vary from country to country, but several common exceptions exist such as allowances for private use, noncommercial purposes, educational activities and research. It is important to note that the specifics of these limitations are determined by national laws. Consulting the relevant legislation, and seeking legal advice, is recommended to understand any limitations that apply in a particular country.

Designs are protected from the moment of their registration with a national or regional IP office. People seeking protection for their designs must file a design application to the office of the territory where they want the design protected.

Design Right Tips

- Prior to applying to register a design, it is recommended a prior art search is performed, to ensure no similar or identical designs exist in the territory where you want your design to be protected.
- Always check the documentation that must be attached to the design application, and its format, as it may vary from one IP office to another.

The registration process, after the application is filed, is country or region specific. In some jurisdictions, the formal examination of the application to ensure it meets all

requirements is followed by a substantive examination to assess the design's novelty and distinctiveness. In others, the substantive examination is not performed; for example, in the European Union, while a substantive phase exists, it is not aimed at checking whether the design is new or possesses individual character, but rather, whether it conforms to public policy and morality standards.

The duration of design rights, as well as the review process, depends on the jurisdiction and the type of protection sought. For this reason, creating a general timeline for design protection would likely be inaccurate, though generally speaking design rights last an initial 5 years from deposit and can be renewed for two further 5-year periods.

Similar to copyright and patents, entities that do not own a design require the owner's consent to legally use it. This takes the form of a license, where the owner specifies the activities the licensee can carry out, and any limitations. If a design owner wants to 'sell' the ownership of the rights, they must assign it to the new owner and update the information with the relevant IP office.

More information on design protection and IP is available on the WIPO website, www.wipo.int/designs/en/ and www.wipo.int/edocs/pubdocs/en/wipo_pub_450_2020.pdf.

A checklist for design rights

- Identify elements of the app that may have design value.
- Determine in what territory you want your design to be registered:
  - Where will you commercialize products embedding the design?
- Based on local law, ensure your design meets all the requirements to be protected in the territory:
- Is it new, distinguishable and ornamental?
- Any other territorial requirement to take into account?
- Seek professional advice to support your application process:
  - Perform a prior art search.
  - Determine the documentation that has to be attached to the application.
- File the design right application and pay the corresponding fees.

- If renewal is allowed, pare the renewal fees:
  - Are you interested in renewing the design rights? If not, you do not need to renew it.

4.6.2. Mobile app's elements that may be protected by design rights

a) Graphic User Interface

User interfaces and their graphical components (icons, graphics, among other things) could be protected as designs if new and distinctive. To get this kind of protection, the design must not be solely dictated by functional considerations, rather it has to be ornamental and also driven by aesthetic reasons.

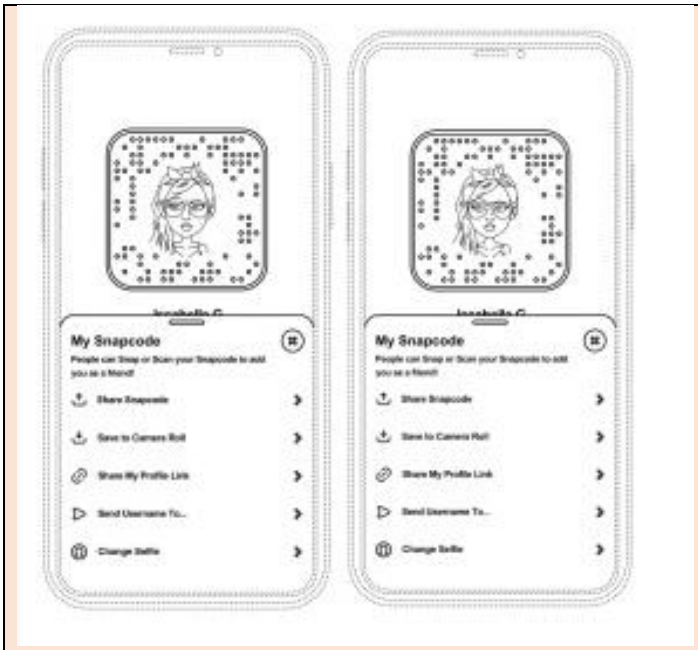
It is worth noting that protecting GUIs as design is not harmonized. While some countries allow for protection as designs, some, China for example, have specific rules on registering user interfaces and others limit the GUI elements that can be registered.[21] For this reason, it is advisable to seek support from local professionals.

Example: Snapchat's designs over GUIs

Snap Inc., the owner of Snapchat, owns several designs of its user interface. Those registered by the company include:

US Design D993270

[21] World Intellectual Property Organization. *Intellectual Property Toolbox for Mobile Applications Developers*. WIPO, 2021: sects. 3.2.3.2, 4.4.2 and 4.4.3.2.



Canadian Design 208780

FIG. 1

4.7. Database rights

To conclude, it is important to make a brief reference to the protection of databases. A full section will not be dedicated to them for one specific reason: database rights are recognized only by specific jurisdictions, mainly the European Union, where the so-called

database sui generis right exists. Other jurisdictions protect databases via copyright if they meet copyright requirements, or trade secrets, or more simply by contractual protection.

The European Union defines databases as a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. Protection is triggered when the creator can prove they have made a substantial investment in obtaining, verifying and/or presenting the database's contents.

The sui generis database right protects the contents of the database, allowing the right holder to prevent others from extracting and re-utilizing the contents without their consent. It lasts 15 years from the creation of the database and does not require registration.

4.8. Conclusions

There is a series of different IP rights that can protect the various elements of mobile application technologies. The important words here are "different IP". Often the concept of intellectual property is used generically, and it is important to distinguish the different assets (or aspects) that may potentially be protected and the different forms of available IP protection. These are summarized in the table below.

Table 4.1 Summary table

IP protection	What it protects?	Duration	Pros	Cons
Copyright	Original literary, dramatic, musical and artistic works (including software).	Generally, copyright protection lasts for the life of the author plus at least 50 years (e.g., in China, Kenya and Philippines). In other countries (e.g., France, Italy, Spain and the United States of America), the duration is the author's life plus 70 years.	Automatic protection Relatively long duration International recognition Free	Limited to expression not ideas
Patents	Inventions, including processes, machines and compositions of matter.	United States of America: 20 years from filing. European Union: 20 years from filing. Others vary.	Extensive exclusive rights Can be commercially valuable Extends to functionality	Expensive Requires disclosure
Trademarks	Symbols, names and slogans used to identify goods or services.	United States of America: 10 years (renewable). European Union: 10 years (renewable). Algeria, Ghana, India, Japan, Kenya, Philippines, South Africa, South Korea, Thailand, Viet Nam: 10 years (renewable). Bahamas: 14 years from registration.	Protects brand identity Renewable indefinitely	Requires active use and renewal
Trade secrets	Confidential business information giving a competitive edge.	As long as it remains secret.	No registration required No duration limit	Requires active technical, legal and organizational protection measures Lost if disclosed Hard to enforce
Designs	Appearance, shape, surface or ornamentation of an object.	European Union and United Kingdom: the initial protection lasts 5 years and can be renewed for additional 5 year periods for a total of 25 years. Chile, China, India, Kenya, South Africa, United States of America: total of 15 years. Japan: 25 years.	Protects aesthetic of product Exclusive rights	Can be limited in scope
Database sui generis	Structure, arrangement and organization of databases.	European Union: 15 years from creation or from date of publication.	Protects against unauthorized extraction or reutilization	Specific to EU Does not protect data itself

Source: Authors.

IP Protection Key takeaways

Most elements of a mobile app may protected by IP rights, including:

- Copyright: protects the expression of ideas, such as source codes, graphics and user interface design. It does not protect the idea itself but how it is expressed.
- Trademarks: protect brand identifiers such as app names, logos and slogans on a territorial level, ensuring no other product/service can cause confusion in the market.
- Patents: protect novel inventions or processes. For mobile apps, this might be a unique algorithm or functionality. They prevent others from making, using, or selling the patented invention.
- Trade secrets: any formula, practice, process, design or compilation of information that gives a competitive edge. Ensure confidential information, such as algorithms or business processes, are not disclosed.
- Designs: protect the visual appearance of a product. In mobile apps, it can be related to icons, or UI/UX design elements, among other things.
- Data: depending on the jurisdiction, databases or specific data compilations might enjoy protection. Understand your rights on data you collect, generate or process.

An IP strategy taking all these elements into account will contribute to a successful mobile app project.

Throughout this handbook, in particular, chapter 7, it is apparent that establishing a clear strategy to identify and protect IP generated in the context of app development is an essential part of business development, and may be a key part of any business strategy.

4.9. Useful links and resources

WIPO, *Protecting your Mobile App: Intellectual Property Solutions*. http://www.wipo.int/publications/en/details.jsp?id=4569

WIPO, *Intellectual Property Toolbox for Mobile Applications Developers*. http://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo_ip_toolbox_mobile_apps.pdf

WIPO, *The Role of Intellectual Property Rights in the Development and Commercialization of Mobile Applications*. http://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo_iprs_mobile_apps.pdf

Gubby, H. *et al*., Intellectual Property and the Protection of Apps in the European Union. *European Journal of Law and Technology Vol 11 No.3 (2020)*. <http://www.ejlt.org/index.php/ejlt/article/download/713/1020/3441 >

Chapter 5. IP contracts in mobile apps

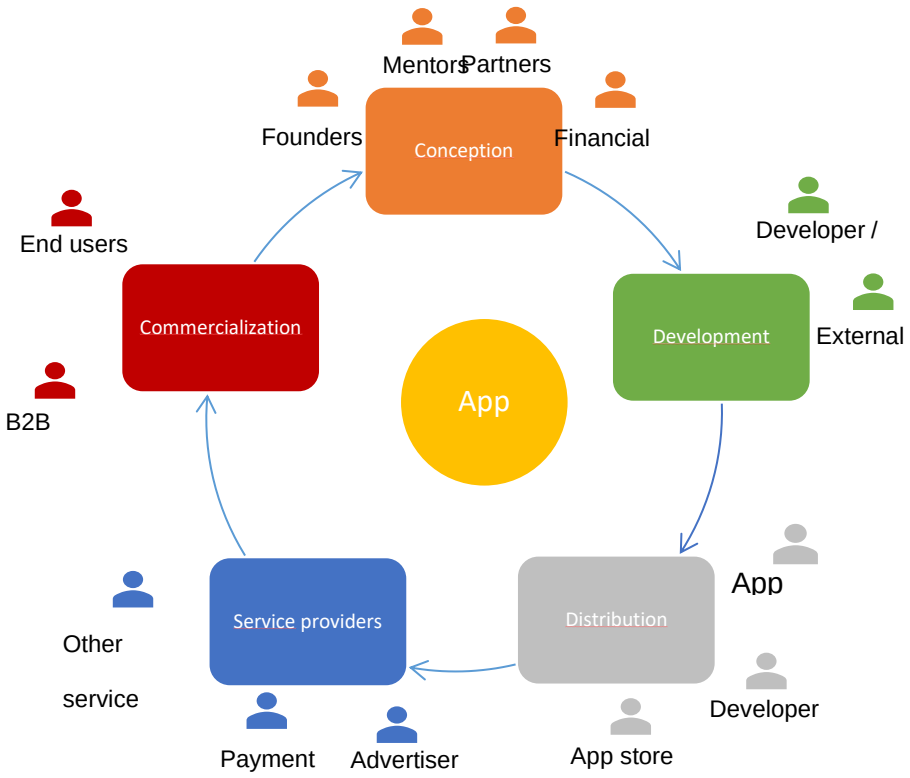
5.1. Introduction

This chapter addresses the contractual framework applicable to entities that design, develop and distribute mobile apps, and focuses on those IP related aspects of those contracts.

The stages of the life cycle (see Figure 5.1 below) were presented in Chapter 2, and the different actors or stakeholders in this cycle, which includes the following:

- conception;
- design and development;
- distribution via the app stores;
- third-party service integration; and
- commercialization to users.

Figure 5.1 Key stakeholders in the life cycle phases of a mobile app



Source: Authors.

This chapter looks at the contractual relationships between these actors. This will familiarize readers with the contractual framework that applies in the typical life cycle of a mobile app, and the issues that may arise, particularly what is necessary to protect and regulate IP. It is important to be aware of the rights to be negotiated and obligations incurred when each of the contracts is formalized, so stakeholders can operate knowing the facts and liabilities and thus avoid contractual disputes that could have an IP, economic or reputational impact.

5.2. App conception

From the moment a mobile app is conceived – a basic idea for the mobile solution, the features it may have and value it brings to users – protecting the information that is generated, as trade secrets or otherwise, is essential to preserve the innovation and competitive position. In fact, throughout all stages of the app's life cycle, strategic information regarding business, strategies, financial situation, assets and technology must be protected from unauthorized access or disclosure.

While technical and organizational measures for safeguarding information are important (and vital for legal protection in some jurisdictions), confidentiality or nondisclosure agreements (NDAs) are also widely used in the software development industry to provide contractual protection measures and enable information sharing within the mobile ecosystem.

5.2.1. Confidential information and nondisclosure agreements

Innovation and creative activities and collaboration among actors for app development and commercialization generate technical and commercial information that is important for the business, including know-how, methods and processes, client and supplier lists, prices and financial information. Protecting this information and managing its access and use are essential for IP, to preserve exclusive use by the owner of the information and authorized third parties. In app development, key information assets include the software

source code, algorithms and methods that may be embedded or implemented in this code, and graphic interfaces. While these assets have different types of formal protection (see chapter 4), they are also information assets of the developer, app developer or third party providing integrated services or other support to the app.

Over and above the need to protect the entity's own confidential information, there may be external motivations to enter into a non disclosure agreement (NDA), such as to comply with confidentiality duties established by law (for example, processing personal data) or with existing obligations to third parties (for example, when sharing information with third parties with whom confidentiality duties have been defined).

NDAs are relevant not just to this stage but throughout the whole app life cycle and among the various actors. Depending on the stage, there are different types of confidential information that must be protected and its use regulated by an NDA between the identified parties.

Table 5.1 Information protected throughout app life cycle and parties involved.

Stage	**Information to protect**	**Parties involved**
Conception–development	App business model and plan App technology architecture App user interface App marketing actions plans App IP strategy Source code of the app and any backend/server side and third-party integrations and interfaces	Founders Contractors Employees Suppliers Consultants Partners
Financing	All information made available to other entities to obtain funds to support the development and commercialization of apps	Investors Banks Lawyers Consultants and entities acting as intermediaries

Distribution	App software: object code shared directly or indirectly with app stores	App store Distributor/reseller/referral partners (residual)/app publisher
Service providers	Technology, interfaces, documentation Samples of the app, GUIs Marketing action plans	Advertisers External software developers Platform services
Commercialization	App software (object code) Backend/server software and technology Product documentation Metadata on app use	End users B2B clients Developers Support and maintenance services

Source: Authors.

Confidential Information Tip:

Protecting information through adequate technical, legal and organizational measures is not just good practice but in some jurisdictions a condition of obtaining trade secret protection.

In an NDA, the key clauses are:

- **Scope**: it is imperative to be precise in defining what is considered confidential among information shared or generated during interaction between parties. This definition should also include what is considered out of scope.
- **Project or purpose definition**: defining the project, or the purpose of sharing the information, will establish boundaries and the reasons why it is being shared.

  Tip:

  Do not always use standard definitions but rather, those that are precisely adapted to the relationship between the parties.
- **Permitted disclosures**: defining entities or individuals to whom disclosures are permitted gives both sides greater control over protecting confidential

information. Sometimes, identification of specific entities, departments and even individuals is fundamental, ensuring confidentiality obligations are passed on.

- **Unilateral or mutual obligations**: each scenario will define when it is of greater advantage to have a unilateral NDA or a bilateral (reciprocal or mutual) one, the latter assigning to both parties the same obligations in respect of each other's confidential information.
- **Duration:** the duration clause defines how long the NDA remains in force (typically one to six years), though the obligations to preserve confidentiality may also be perpetual.
- **Liabilities**: defining the consequences of disclosure is essential in order to not accept limitations that may rid the infringer of liability, and to ensure adequate protection and protection measures (for example, requesting preliminary injunctions to prevent further disclosure).

In many jurisdictions, damages relating to confidential information are considered indirect damage, so this should not be excluded.

Tip: technical protection measures

NDAs should impose technical and organizational protection. In the absence of such measures (encryption, approval, registration and continuous updating of the recipients of confidential information, and procedures for security breaches) you may find yourself with an NDA with dubious enforceability.

An example of Non Disclosure Agreement provided by WIPO can be found online at http://www.wipo.int/amc/en/docs/ipagmultinda.doc.

Checklist: protecting and sharing confidential information

Initial internal protection:

- Which information has value for the entity?
- Has the company taken appropriate actions to prove ownership, content and date of creation of the information?
- Has the company taken appropriate technical and organizational action to protect unauthorized access, use or disclosure?

Sharing information:

- Who is this information going to be shared with, and for what purpose?
- Can you determine if they are reliable and how they manage confidential information?
- Who else needs access to fulfill the defined purpose of sharing any information (for example, advisers, consultants, partners)?
- According to the type of information, should specific technical or organizational measures be defined to reduce risk (for example, for source code)?
- For how long may third parties retain the information, and should they delete or return it at the end of the relationship?

5.3. App design and development phase

In the app life cycle, one of the determining phases is the design and development of the app, in which different parties may be involved, from the app developer (in-house development) to third-party software development companies (often called agencies) and third parties that bring or link technology to the app or its backend/server side.

So an app can be developed either by a company's internal employees or by third-party developers. In-house development offers greater control of the IP, confidentiality and internal collaboration, but can be costly and may lack specific expertise. From an IP perspective, in some jurisdictions, if an app is created by an employee, the IP rights automatically belong to the employer. However, it is advisable to explicitly cover the IP assignment to the company in employment contracts in case the law changes or questions arise on whether the employee created the code during their employment.

Outsourcing to third-party agencies can be cost-effective, time efficient and provide access to specialized skills, but it requires effective communication and information security measures, and correct management of IP.

5.3.1. IP agreements

When apps are developed by independent companies or contractors, the assignment or even licensing of IP is not typically automatic. To secure ownership of sufficient IP rights, the commissioning app owner should obtain a license or assignment of these rights from the developer. This can – and should – be done via a separate written agreement, called a license or an assignment (sale) agreement, or as part of the overall software development agreement (see section 3.2). Regardless of the method, certain considerations and key clauses apply to regulation of IP rights transfer.

In the design and development phase, developers need to be aware of two legal terms that are important when discussing IP ownership and exploitation: licensing of rights and assignment of rights. The choice between assigning or licensing the IP of an app depends on the goals and preferences of the developer.

Table 5.2 Comparison, licensing vs. assignment of IP

	Licensing	**Assignment**
Meaning	Grant the right to use the IP. Such rights are often subject to restrictions and limits.	Transfer of IP ownership.
Ownership	Retained by the software development agency, control of IP is preserved.	Relinquished – control is in the hands of the app developer (assignee).
Moral rights transfer	No transfer or waiver.	Depends on jurisdiction.[a]
Liabilities and responsibilities	The software development agency is responsible for potential IP or technology disputes or support obligations.	Developer may be relieved of IP-related obligations, as the assignee is now the owner.
Pros (app owner perspective)	The software development agency retains ownership and the technology may be licensed again (non-exclusive license).	The software development agency transfers ownership to the Developer, avoiding future liabilities and responsibilities related to the IP.

	Recurring revenue through licensing agreements.	Upfront payment for IP transfer.
Cons (app owner perspective)	The software development agency may face potential disputes if the licensing terms are not clearly defined or if the licensee breaches the agreement.	The software development agency loses control over the app's IP and cannot use or modify it further without permission

[a] World Intellectual Property Organization. *Understanding Copyright and Related Rights*. WIPO, 2016. <www.wipo.int/edocs/pubdocs/en/wipo_pub_909_2016.pdf>.

Source: Authors.

Software development agencies usually prefer to license the developed software to the app owner rather than assigning their IP rights, given this allows them to reuse code and build a library of components for other clients. The app owner, however, ideally wants the IP assigned, giving them complete ownership of the software they have paid to have developed. With correct IP assignment, the app owner can fully exploit the app software, making it available to users, adapting and evolving it, or selling or licensing it, without violating any IP rights. Under a licensing arrangement, making future changes to the app may require the IP owner's consent, which could involve recurring license fees.

To safeguard their interests, the app owner should aim for an IP assignment in developed code. But a software development agency may say it cannot assign IP rights because the app created for a customer incorporates some of the agency's standard code bank, which has already been used for other customers. In this case, the app owner requires a license for these reused components.

In some jurisdictions, the price for IP assignment or license is charged separately from development work. The app owner is considered to be buying two different products. In other jurisdictions, a single price is charged that includes the assignment or license. Care must be taken to clarify which of these regimes applies to a specific contract or agreement to avoid unexpected claims for additional compensation, a point that may need to be clarified in the wording of the agreement. Tax issues may also arise, so specialized advice should be considered.

To clarify the IP rights and their management, it is useful to distinguish between prior work that the agency is bringing to the app (background IP such as software development kits or tools), in which its IP rights exist before a project starts, and new developments or creations (foreground IP, including new code or client specific designs or methods) created during development of the project and which are often specific to the app. As discussed, the developer should negotiate to take an assignment of foreground IP, and a sufficiently wide license to background IP, freeing them to operate and sell the app.

If the app owner cannot obtain the assignment of all IP rights in the app, and is required to take a license for part or all of it (a licensing agreement), the app owner should ensure the following to permit the widest usage rights possible:

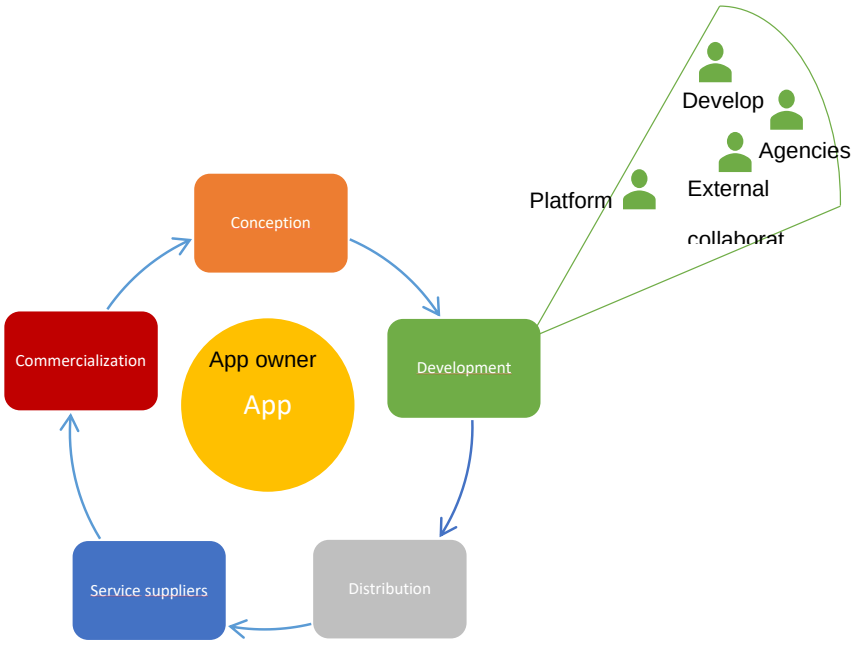
- worldwide rights, that are unlimited in time and transferable to third parties;
- rights to transform or adapt the software (with access to source code);
- rights to sublicense the technology to another party (for example, where another developer specializes in a different platform or app store); and
- rights to take legal action and pursue claims against third parties who infringe IP in the app.

5.3.2. Software development agreements

From a legal perspective, when third-party agencies develop the app, it is necessary to formalize a software development contract that regulates the obligations and responsibilities of the parties, as well as other essential issues, to guarantee development of the agreed app.

While the software development contract is usually formalized between the agency/agencies and the app owner, there are other stakeholders involved in the app development phase.

Figure 5.2 Stakeholders during the Development stage



Source: Authors.

Key clauses of the Software development agreement include:

- **Scope and deliverables**: identification of the software to be developed, architecture, functionalities, integrations and data management, among other things. The agreement should specify what the agency is expected to deliver on completion of the app. This includes detailing the app's components, which may encompass the agency's software, bespoke software crafted by the agency for the developer, approved third-party software or open-source software. The agreement must also define what documentation will accompany the software to explain the app's functionality, as well as list any other work or services expected from the agency.
- **Background**: dependencies and background IP that the developer may bring to the table, to avoid any later dispute over ownership and IP rights.
- **Testing and acceptance**: process to demonstrate and validate that the app and its elements work and conform to the business priorities identified by the

developer and interoperate with any third-party services. This will often involve making the app available on a beta basis, either on a simulator, on the actual device, or even through the app store.

- **Methodology**: software may be developed using a traditional waterfall methodology, or a more modern agile delivery method. The contract should indicate and regulate this method, given the significant differences (see table 5.3 at the end of the list), and outline the pros and cons of the different methodologies.
- **Third-party/open-source components**: the use of third-party components in software development, both proprietary and open source, carries multiple legal implications for developers. Consideration should be given to:
  - liability arising from use of these components;
  - maintenance and availability of third-party components;
  - if the software is intended for commercial use, whether the third-party license allows for sublicensing;
  - license compatibility between the third-party component and their own software; and
  - international export control laws and regulations. For more information on integrating open-source components, see chapter 9.
- **Delivery**: the agency can deliver the app by transferring it to the developer, or by uploading it directly to the app store on behalf of the app owner. Bespoke software should be delivered in source and object code, and the remaining non-source code should be escrowed, unless it is part of a reliable third-party framework that is expected to be available indefinitely. Compilation instructions are necessary, and provision must be made for managing the cryptographic keys used to sign the code.

Tip: When an agency manages the relationship and account with app stores, a procedure for credential management must be defined with the app owner. This will avoid tension and the eventual retention of the credentials in the event of disputes.

- **Transition to another developer/agency**: during development, circumstances may arise that prevent the development agency from continuing development; for example, if the agency defaults, becomes insolvent or loses the right to upload it to the app store. It may be necessary to transition the app development in the development contract. It is important to prepare for these circumstances by including a transition and exit plan, with either direct access to the source code in the agency's repository or by using a third-party service (escrow agent) for this access. This scenario is regulated through escrow agreements that provide a tool for use by the developer to continue maintaining the app, on its own or through a third party
- **Compliance**: the agency must comply with the third-party terms and conditions (app store or service providers), regulatory compliance with laws such as privacy and data protection and export control, and security compliance with standards set out in the agreement.
- **Warranties, indemnities and limitation of liability**: it is important to consider whether the warranties, indemnities and limitation of liability of, for example, the agency in charge of developing the app, are regulated, considering two relevant aspects:
  - who holds the IP in the app and access to source (for modification and corrections); and

- the elements of background or third-party code (codecs, game engines) or bespoke (foreground IP).[22]

- **Maintenance and updates**: any arrangement requiring the agency to support the app after delivery of the software must be specified in detail, together with the required service levels and service credit mechanisms. This may include first-line support (support to end users) and handling of queries from the app store.

Table 5.3 Comparison of software development methodologies

Aspect	Waterfall methodology	Agile methodology
Development approach	Linear, sequential process. The requirements for the app must be specified by the developer at the outset, together with relevant milestones, acceptance tests and delivery dates.	Iterative and incremental process, allowing the specifications to change as the app is developed.
Pros	Structured and predictable. Clear documentation and milestones. Suitable for well-defined projects.	Flexibility and adaptability to changing requirements. Quicker feedback loops and customer collaboration. Delivering value early and continuously.
Cons	Lack of flexibility for changes. Challenging to incorporate late-stage revisions. Slow to respond to changing requirements.	May lead to scope creep or difficulties in estimation. Requires strong collaboration and communication. May not suit all project types or teams.

Source: Authors.

Checklist: app software development agreement

- Define the scope of work and deliverables.
- Define the work methodology.
- Define the calendar and milestones.
- Define the acceptance process and criteria.

[22] For more information see, World Intellectual Property Organization. *WIPO Handbook on Key Contracts for Mobile Applications: A Developer's Perspective*. WIPO, 2020: chap. 4.

- Define who uploads and tests in the app store, and manages the credentials.
- Specify known technologies to be used (language, libraries, among others).
- Regulate the use of open-source software (for example, prohibited licenses).
- Define the software source-code repository and access.
- Clearly establish the IP regulation (ownership, licensing, assignment).
- Define a transition out/exit strategy and continuity.
- Define guarantees and ongoing support and maintenance obligations.

Case study: Nintendo and ROM emulation

Renowned videogame company Nintendo has been involved in multiple legal battles regarding the unauthorized distribution and emulation of its games. ROMs (read-only memory) are digital copies of games that can be played on computer systems through emulation software.

Developers and websites that host ROMs of Nintendo games have faced legal action from the company for copyright infringement. Nintendo has argued that the distribution of ROMs and the use of its copyrighted games without permission violates its IP rights.

Legal action has resulted in several ROM-hosting websites being shut down and developers held liable for copyright infringement.

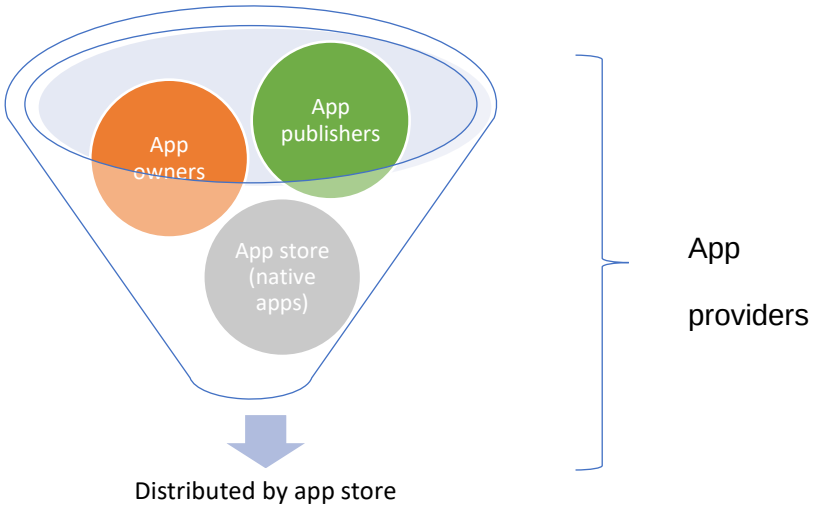
5.4. App distribution

In this section, the focus is the regulation of channels for distributing mobile apps such as distribution contracts. The relevance of app stores' roles will be addressed, and the main controversies that can arise when negotiating with them. A checklist is provided, summarizing the essential IP issues that need to be considered when distributing a mobile app.

The commercialization chain in the mobile app ecosystem is not as large or as atomized as in the rest of the software landscape. Mobile apps are distributed to end users mostly through app stores and, to a lesser extent, from some open repositories and even sometimes directly from the app owner's own website.

Due to the market share they represent, we will focus on app stores for distribution. First, app owners must be aware that app stores own some of the apps they distribute (native apps) but also distribute apps on behalf of app publishers. App publishers may in turn be distributors of other app owners. Hereinafter, they will be referred to indistinctly as app providers.

Figure 5.3 Typical distribution model



Source: Authors.

App stores usually impose their own terms of the distribution. The distribution agreement may include, within the same document: (1) terms of use of the app store site, (2) terms on which the app store's own apps are licensed (essentially as a default set of terms), and (3) other terms to protect the app store as a software distributor.

App stores often give app providers a choice between licensing their apps to end users on the app store's default terms or introducing their own terms. An end-user license agreement (EULA) can be used by the developer in place of an app store's default terms, (or if there are no app store default terms).

The distribution agreement of most app stores is available on their websites.[23] Key contractual issues and clauses are discussed below.

- The app store will be responsible for delivering the app to the end user and will generally also take payment for it, and for any upgrades or in-app purchases. While this is a convenient service for app owners, in particular SMBs, exclusivity on in-app payment methods has resulted in claims related to monopolistic behavior. For further information, see the Apple vs. Epic Games case study below.
- App stores generally choose to characterize themselves contractually as agents, making sales on behalf of the app provider to avoid being subject to certain consumer law requirements. This means that app owners will essentially be selling their products on the app store's standard terms. In reality, the sale process will be entirely controlled by the app store.[24]

The terms of app store distribution agreements are almost always imposed by the app stores, so app owners can rarely negotiate them, except, for example, when that the app has a relevant level of recognition in the market as a top-ranked app, or similar. Besides, every app owner must be aware of granted rights and conditions to decide on protective actions to mitigate any disparities that may arise:

- **Licensing distribution rights**: app providers need to understand the extent of rights granted to app stores. Generally, they are licensing the distribution rights on a nonexclusive basis but should beware of (and reject) unilateral clauses that may establish an assignment or an exclusive license to the app store.

---

[23] Apple: https://developer.apple.com/support/terms/ and Google: https://play.google/developer-distribution-agreement.html

[24] Apple Developer. "Schedule 2: Appointment of Agent and Commissionaire." *apple.com*. Apple Inc. https://developer.apple.com/support/downloads/terms/schedules/Schedule-2-and-3-20230828-English.pdf

- **App store development of competing apps**: app stores tend to reserve the right to develop competing apps or allow competing third-party apps.
- **Warranties from developers to app stores**: app stores expect certain warranties from app providers in relation to the IP in their apps. This includes specifying whether the organization owns the IP itself or whether third-party materials have been used. To be compliant, app providers should have the assignment or licensing chain controlled and updated. Other warranties may be expected relating to compliance with applicable laws, and with the developer's obligations as principal to the end user, in which case the store's legal position is likely to be that of agent, not distributor or reseller.
- **Open source**: app stores may have provisions limiting or demanding additional actions regarding certain open-source components. These must be considered carefully. App providers must check licensing compliance and compatibility to avoid breaching the contract and infringing third-party rights (see chapter 9 for more information

Extract, Apple's Apple Developer Program License Agreement

"3.3.22 If Your Application or Your Corresponding Product includes any FOSS, You agree to comply with all applicable FOSS licensing terms. You also agree not to use any FOSS in the development of Your Application or Your Corresponding Product in such a way that would cause the non-FOSS portions of the Apple Software to be subject to any FOSS licensing terms or obligations."

Note: FOSS means free and open-source software.

Source: https://developer.apple.com/support/downloads/terms/apple-developer-program/Apple-Developer-Program-License-Agreement-20230828-English-UK.pdf

- **Limited warranties granted for app provider**: App stores generally provide limited warranties. Use of their platforms is on an 'as is' basis. App providers need to be aware that damages, including failure and data loss through use of

platforms, are not usually covered. App stores also reserve the right to change, suspend, remove or disable access to any services at any time without notice. App providers and developers must be aware that their apps are subject to removal without notice, and in most cases without compensation.

- **Sensitive content**: a source of frequent concern. App stores are mindful of maintaining their reputation in all the territories where they operate, bearing in mind that what appears harmless in one jurisdiction may be objectionable in another. App providers should ascertain an app store's attitude towards age ratings and ensure the content of its app is always appropriate for the rating it receives.
- **Advertising**: control over creative content, licensing of images and characters, among other things. Some app stores demand wide-ranging rights to include visual elements in the app, including characters, videos of gameplay or the developer's branding images such as logos and trademarks. This right extends to the use of the app on any device, in the app store itself or in its advertising. App store uses could negatively affect the the developer's advertising strategy and brand reputation.
- **Termination**: the developer should consider how easily the distribution agreement can be terminated and its app removed from the app store. It also needs to identify post-termination consequences in advance.
- **Assignment**: app stores do not usually allow a distributor agreement to be assigned, or delegated, in whole or in part, even by operation of law, merger or any other means without their prior written consent. Any attempted assignment without consent will be null and void.

While these distribution agreements (app store agreements) are standard, and difficult if not impossible to negotiate, there are several important issues that app owners should consider at this stage:

- **Who has the relationship with the app store, the developer or the agency?:** is the app being licensed directly by the developer, or is the developer acting as a distributor for a third-party app? Some app stores have one set of terms for individual developers and another for developer organizations. Developers should verify that the correct terms are being considered.
- **How to respond quickly to app store takedowns**: app stores can and do remove apps for various legal failures. These include infringements of the IP of any third party (or a threat of such infringement), any other breach of third-party rights and failure to comply with applicable laws. The approach is often "withdraw first, deal with the issue later". This places the app provider in a potentially risky position, in terms of lost revenue and reputation. Most app stores have a procedure for receiving complaints of legal infringements but no process for investigating them or conducting additional vetting. App providers must ensure written approval, on time, to avoid breaching a contract.

Recommendations for app owners

In relation to illegal content and complaints, app owners should:

- Draft a policy to quickly answer app stores to avoid time wasting.
- Define a series of documents that will assist in answering a complaint with IP rights and contracts.
- Keep up to date on the terms of the applicable distribution agreement.
- Seek specialized legal advice.

- **Cost of in-app purchases**: app stores charge service fees to process in-app purchases by end users. App owners need to clarify the cost and scale of such fees. These charges are not uniform across all app stores. Close attention must be paid to the specific app store's terms. Please review Case Study Apple vs Epic Games to be aware of status.

Checklist: reviewing app store distribution agreements

- Periodically review the terms of the distribution agreement for each app store.
- Pay close attention to what is being given to the app store (ownership rights, a perpetual license). Act to adapt licensing strategies and internal processes to the provisions of the distribution agreements.
- Implement a policy with procedures to respond to take-down notices.
- Determine how easy it is to terminate the agreement and remove the app from the app store.
- Pay attention to in-app purchase fees and other commissions to be charged.

Case study: Apple vs. Epic Games – App Store policies and In-App Purchases

In 2020, Epic Games, the creator of the popular Fortnite, introduced a direct payment system within their iOS app, bypassing Apple's in-app purchase system. This violated Apple's App Store guidelines, which require developers to use the Apple system and pay a 30 per cent commission on purchases. Apple responded by removing Fortnite from the App Store, prompting Epic Games to file a lawsuit in the Northern District Court of California, alleging antitrust violations and monopolistic behavior. The case involved complex legal argument over Apple's control of the App Store and the fairness of its policies. The legal battle drew significant attention from the tech industry and raised broader discussions about app store regulations and the relationship between developers and platform providers.

The US Court of Appeals for the Ninth Circuit confirmed this position in its 2023 decision: there must be an option to direct users to a payment method hosted on an external website. This way, app owners can avoid the store's 30 per cent recurring payment fee.

5.5. Commercialization to end users

This final section focuses on the commercialization of mobile apps to end users. It discusses the key aspects of the end-user license agreement (EULA), highlighting the main clauses that should be incorporated. The implications in regulated areas such as consumer services will also be addressed. Finally, app stores requirements will be

considered in relation to regulating the use of mobile apps through the EULA. To facilitate understanding and the application of these concepts, a checklist is provided.

As detailed in chapter 4, an app can be protected by copyright in most jurisdictions under local legislation. Where this is the case, end users need a license to install and use the software on their mobile devices to avoid any infringement. These licenses are generally referred to EULAs which allow app owners to protect their asset by setting restrictions on the use of their apps and providing a framework for user compliance.

Developers define their liability in the EULA, limiting it as much as they can. This practice finds counterbalance in mandatory law, especially consumer law. Many jurisdictions, assuming a power disbalance in negotiation, have legislation protecting consumers by restricting the extent to which liability can be contractually limited.

Example: Standard EULA, Apple App Store

Apps made available through Apple App Store are licensed to you, not sold. The license to each app is subject to prior acceptance of a standard end-user license agreement or, if one is provided, a custom end-user license agreement. The license to any Apple app under this standard EULA or custom EULA is granted by Apple, the license to any third-party app by the app provider of that third-party App. Any app subject to the standard EULA is herein referred to as the licensed application. The app provider or Apple, as applicable (the licensor), reserves all rights in and to the licensed application not expressly granted under the standard EULA.

Source: Apple Inc. “Licensed application end user license agreement.” Terms dated Jan. 8, 2023. <www.apple.com/legal/internet-services/itunes/dev/stdeula/>.

Common important clauses in a EULA are:

- **Acceptance**: this clause defines when a EULA is contractually binding
  - Providing legal terms before purchasing: providing a link to the EULA on the purchase page of the app store, so the acceptance process is informed.

- Providing legal terms after payment: requiring end users to accept the EULA before installing an application. This is not generally considered a good practice as payment is made without the necessary information.

Local laws should be checked: many countries (e.g. Spain) require a user to take an express action (e.g. clicking a box) to signify their acceptance of the legal terms. If not, this may affect the enforceability of the EULA against the user.

- **Conflicting terms**: given app store terms and app provider terms may coexist, interpretation of contradictory clauses must be defined. App stores tend to prevail over corresponding EULAs. To mitigate or avoid conflict, app providers should identify conflicting terms and rewrite their EULAs to reflect a position that is acceptable to them.
- **Restrictions**: developers should include several types of restriction in any contract with the end user, including:
  - standard clause limiting rights to download, install and use the software;
  - age requirements;
  - transferability; and
  - acceptable uses.
- **Support services**: app stores require developers to take responsibility for quality issues through their support services, with contact details provided to end users. Such services may in some cases be outsourced to an agency. Applicable legislation should also be checked to ensure that other required information, such as a toll-free number or email address, has been properly published with an app.
- **Limits to liability of app owners**: end users might be unable to access or use an app or service for various reasons, including errors, defects, interruptions or delays. Common causes include:

- Reduced service levels, defects attributable to third-party services, damaged hardware or software, or loss of data stored on the device.
- Limited functionality as defined in technical documents.
- Removal of certain information by the app store.
- Disclaimer regarding accuracy of financial information or location data displayed through the app, or on a service or linked third-party site or service.

Some of these disclaimers and limits may be validly established by the app owner but they may not always be able to cap their financial liability, e.g. to consumers, as local mandatory laws may prevent or limit their ability to do so. While it may not be possible to disclaim all liability, educating the user about the uses and limitations of an app will be desirable. Developers should check if any further information is required by consumer laws or other applicable rules.

Attention to consumer laws

App providers should seek advice on other consumer laws that may apply to users of their apps. Depending on the jurisdiction, contracts may have to be presented in all of a country's official languages or include provisions allowing the user to terminate the agreement within a cooling-off period (though possibly exempting digital goods delivered for use immediately, which include apps). It is also important to be aware that many countries have legislation that requires services to make provision for users with disabilities, which could entail service providers adhering to particular standards or making reasonable adjustments.

For example, an app that provides wellness recommendations for a person's preferences and lifestyle, for instance, could feature a disclaimer: "This app is designed for entertainment only. It is not intended to give medical or health advice, and you should always consult a qualified medical expert." Such language is more likely to be effective than: "We accept no liability for loss or injury caused by this app." The rules in this regard vary significantly from jurisdiction to jurisdiction.

- **Alternative dispute resolution (ADR)**: is a process where an independent body considers the facts of a dispute and seeks to resolve it, without the parties having to go to court. Increasingly, consumer laws in many countries require app providers to resort to a recognized ADR entity. The provider must reference the entity's name and website address in their terms and conditions. Users not satisfied with the outcome of ADR can still go to court. Applicable legislation must be checked to see if such requirements apply. Even where not legally mandated, ADR can be a useful way to resolve disputes, particularly with users. The WIPO ADR service provides one such option (for detailed information on ADR, see chapter 6).

5.6. Licensing apps to third parties

This section focuses on the commercialization of mobile apps to third parties. It discusses the key aspects of different licensing agreements and the main clauses that developers should incorporate. To facilitate understanding and application of the concepts, a checklist is provided.

Once an application has been created, developers may decide to sign licensing agreements with interested third parties, not as an end user but as part of their business activities. This model is known as business-to-business-to-consumer (B2B2C), in which developers grant rights to third parties to use, include or modify a technology or product for the third party to offer another service or product in the market.

Two principal licensing models can be identified, which are commented next:

1. Licensing app-related technology to app developers; and
2. Licensing white label apps or services.

5.6.1. Licensing to other developers

The app owner may license rights to use its technology to a third party so that the latter can include this technology, mainly through a SDK (software development kit), in the

licensee's product. In this model, the third party may already have a software or will have to develop what is referred to as an integrated product.

Example: location based technologies
An app owner of a sophisticated location-based service licenses this service to other third parties who can then integrate it into their apps. This allows these companies to offer location-based services in their apps without having to develop them from scratch.

Key clauses of a B2B app license agreement will include:

- **Granted rights**: the app owner grants the rights on a nonexclusive basis to use and reproduce the technology, but only in order to incorporate, embed, interface, link or otherwise integrate for implementation with or into the third party's technology to create a product. The developer grants the right to distribute and sublicense use of the integrated product to clients as part of the third-party products/service offerings.
- **Restrictions**: the app owner explicitly restricts software distribution as part of the integrated product.
- **Warranty**: the app owner limits warranties to the technology licensed, not the integrated product.
- **Support services**: as a technology supplier, support services are normally provided by the licensee, not the developer.

For further information, see assignment and licensing section.

5.6.2. White label product

The app developer licenses rights to a third party to label, use and distribute a product with the third party's brand name. In this model, the third-party licensee is interested in providing some service to the market and does not have the software to do so. However, it needs to use its own trademark to label the product.

In general terms, the developer can license just the backend of the app or a full application with both server and client sides.

Example: white label app for hotel clients

An app owner in the building automation sector licenses a mobile app and platform solution to hotels (clients) to allow them to provide services to their guests (end users) under the hotel chain branding. Through the technology, the hotel allows its guests to manage access to their rooms and to certain devices inside the rooms.

Key clauses of the white label agreement will be.

- **Granted rights**: the app owner grants limited rights to rebrand and distribute licensed software to third-party clients.
- **Additional terms**: the app owner includes some minimum terms and conditions that must be included in the corresponding third party's EULA.
- **Noncompete**: a restriction to develop competing products may be imposed on the licensee.
- **Warranty**: a standard software warranty is provided by the app owner.
- **Support services**: acting as product supplier, the app owner provides support services on the core code and maybe integrations made for the white label partner, who then deals with first level support for end users.

Checklist: developers and license agreements

- Understand and be aware of different licensing models.
- Restrict licensee use of technology to their own business clients.
- Negotiate minimum terms for the third party's EULA.
- Be aware of warranties as they vary substantially through the different license models.
- As the licensee will have access to relevant information, define strict confidentiality obligations.
- Consider developing an SDK in an open-source permissive license to facilitate implementation.

5.7. Service provider agreements

Apps may require integration with other services to enrich their functionality, as opposed to building them from scratch. Common examples include advertising services, payment services, third-party data feeds and social media, such as social networks, comments and maps. More sophisticated services include visual recognition functionality, data analytics, wallets, smart keyboard and blockchain services. Integration is achieved via application programming interfaces (APIs), a defined method of communication between various software components with a set of subroutine definitions, tools and protocols. These give a mobile app borrowing functionality and allow it to use data from other apps or services.

Here we look at several important contracts regarding mobile apps and service providers.

5.7.1. Service providers in general

Some general comments can be provided regarding third-party service agreements, including the following points:

- **Reliable suppliers**: choosing the right service provider is a crucial decision that can have long-term consequences. To avoid the need to migrate to another provider, and service disruption, developers should at the beginning of the project ensure their chosen provider is able to scale up as the business grows. This is why a due diligence should be done prior to the engagement.
- **Critical service providers**: where a third-party service is critical to an app's functionality, it is also wise to consider providing an alternative with similar functionality. A backup service provider can be kept on standby in case the original supplier ceases operations or suspends service for any reason. This applies particularly to payment services, but it can also be relevant to geographic information, mapping, data feeds or other services.

Once the provider has been chosen, some important clauses to look out for in this relationship include:

- **Scope of service**: it is necessary to define in full the services covered by the contract and, as far as possible, those outside the contract. This will be particularly relevant in critical situations where the expectations of the parties may be in opposition.
- **Integration**: many third-party services need to be integrated into the app, or the backend on the cloud server. The contract should set out how this is done, the testing process and the support given by the provider on the integration.
- **Licensing**: third-party services are usually IP based, with software or interfaces embedded in the app or included or linked to the backend. This means obtaining a license to use the technology, in the manner defined by the relationship; for example, licensing an SDK to embed in the app, with royalties per use, per time, one-off, or per quantity of data transmitted, among other things.
- **Changes to service**: a procedure should be defined to accommodate the service proposal to the new needs of the parties or those arising from the market. Providing mechanisms that provide flexibility from the outset will help parties to redirect the contract without the need to break it.
- **Service level agreements (SLAs)**: under standard third-party agreements, providers do not usually enter service-level commitments, but SLAs may be negotiable at additional cost. This is the time for developers to look closely at service levels and commitments concerning uptime and availability, which will have a direct impact on the quality and level of service offered.
- **Reps and warranties**: many providers tend to either exclude or limit their warranties and liability concerning data loss, corruption and service failure. In contrast, such service agreements have traditionally often included provisions for indemnities demanded by providers for customers. These indemnities aim to

cover third-party claims and breaches of acceptable use policies or data protection laws, primarily due to the responsibilities data processors must undertake under GDPR. But the landscape is changing due to increased competition, and, to attract more customers, providers are offering SLAs, warranties and indemnities. This shift in the customer/supplier relationship means that when considering services of a relatively standard nature, it is essential to evaluate not only the quality and cost but also the favorable terms offered by each provider.

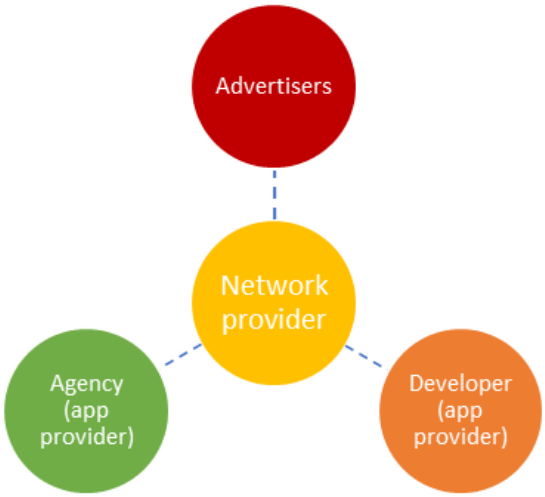
- **Transition period and services**: termination of a contract may be critical for one or both parties. Defining a transition period in which there will be continuity of services is essential so the developer's operations are not affected. The definition of a price applicable during the transition, as well as a term that adjusts to the real needs is highly recommended.

5.7.2. Advertising agreements

Many apps integrate advertising services, most being third-party advertisers. When app providers decide to display ads in their apps, they need an advertiser to provide them with a suitable feed. There are many such providers and, more importantly, many advertisers interested in displaying their ads. These are usually managed by an ad network provider.

Commercially, the ad network provider's portfolio of advertisers and its reputation will be analyzed; the more customers it has, the more consistent and predictable its commercial strategy.

Figure 5.4 Stakeholders in an advertising network



Source: Authors.

As mentioned, network terms are almost always imposed by the network providers, but with increased atomization, significant differences exist between each term. The app owner must be aware of granted rights and conditions to decide on protective action to mitigate any disparities that may arise. The following are the main issues facing developers when considering the conditions under which advertising networks operate:

- **App owner's content access**: the app owner typically grants network providers the right to access, index and cache requests for their content.
- **Advertiser's selection and management**: the network provider has the sole right to enter into agreements with advertisers and modify portfolios. The only possible exception is age-range limits.
- **Compliance of local laws and policies**: the app owner is ultimately responsible for complying with applicable laws and regulations, including privacy regulations.
- **Minors and privacy**: content/apps, in most cases, can only be made available to minors with written notification to the network provider. Some ad networks prohibit advertising to minors altogether.
- **Data generated by ads**: each party owns the data it collects, including data on end users.

- **Payment terms**: the app owner must understand the payment terms offered (to be made within 30 or 60 days) and the minimum payment thresholds that may apply.
- **Termination and modification**: ad networks will often insist on the right to terminate the service unilaterally, at their discretion. They also often have the right, at their discretion, to unilaterally modify, suspend or discontinue services or to suspend access to an account.
- **Warranties**: the standard terms of most ad networks provide a service with limited warranties, on an 'as is' and 'as available' basis, often with no obligation to provide support or updates.
- **Indemnities in place**: under their standardized contracts, ad networks generally have extensive indemnities to their own advantage, with few that are mutual.
- **Limitation of liability**: limits operate in favor of the ad networks and are designed to be as wide as legally permissible. They often exclude liability to the maximum extent allowed by law and limit the ad network's liability to a contractual sum. Liability payments may include a fixed sum or a percentage of the net annual amount payable by the network provider.

Checklist for advertising network agreements

- Review the ad network's proposed contract in detail – even if there is no room for negotiation – to be aware of onerous clauses.
- Pay special attention to target definition in order to align with app stores and avoid suspension of services related to inappropriate advertising.
- Reserve rights to exclude advertisers.
- Keep updated on the terms of the applicable distribution agreement.
- Seek specialized legal advice.

5.8. Conclusions

The contractual framework applicable in the life cycle of a mobile app has been discussed, including a review of the main contracts, and the rights, obligations and other issues that may arise. There has been a focus on IP management and regulation, given IP is a strategic element of the ecosystem**.**

It is important app developers and owners, in particular, are aware of the rights to be negotiated and the obligations incurred when each of these contracts is formalized, so stakeholders can negotiate their position in full knowledge of the facts and liabilities, and thus avoid contractual disputes that could have an IP, economic and reputational impact. The ability to negotiate the terms of these agreements is often reduced, if not eliminated, when dealing with platforms and app stores, who offer their services under standard and non-negotiable terms.

Finally, the end user is a key player in the system, but, again, their contractual relationship with app owners and app stores is that of the weaker party, with non-negotiated terms – and for this, legislators often step in with strict consumer protection laws.

App sector contracts: Key takeaways

App development and commercialization requires the involvement of many actors, from developer to end user.

These actors are linked by contractual relationships that manage the different aspects of the technologies and app services.

The key relationships are:

- app developer to app owner: for provision of mobile app development services;
- app owner to app store: for publication of the app, mainly under the standard terms of the app store;
- app owner to end user: the EULA for use of the mobile app; and
- end user to app store: to access and use the store to download mobile apps and any updates.

From an IP perspective, these contracts regulate the creation, protection, use and enforcement of IP rights, making them strategically important.

5.9. Useful links and resources

WIPO, *WIPO Handbook on Key Contracts for Mobile Applications: A Developer's Perspective*.http://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo_handbook_key_contracts_mobile_apps.pdf

WIPO, Multilateral Confidentiality Agreement. http://www.wipo.int/amc/en/docs/ipagmultinda.doc

Chapter 6. IP dispute resolution

6.1. Introduction

This chapter describes potential means for resolving disputes related to mobile apps and focuses on IP-related dispute resolution mechanisms, namely judicial procedures, principally focusing on the law to determine jurisdiction and alternative dispute resolution (ADR), and on which procedure to choose, and how.

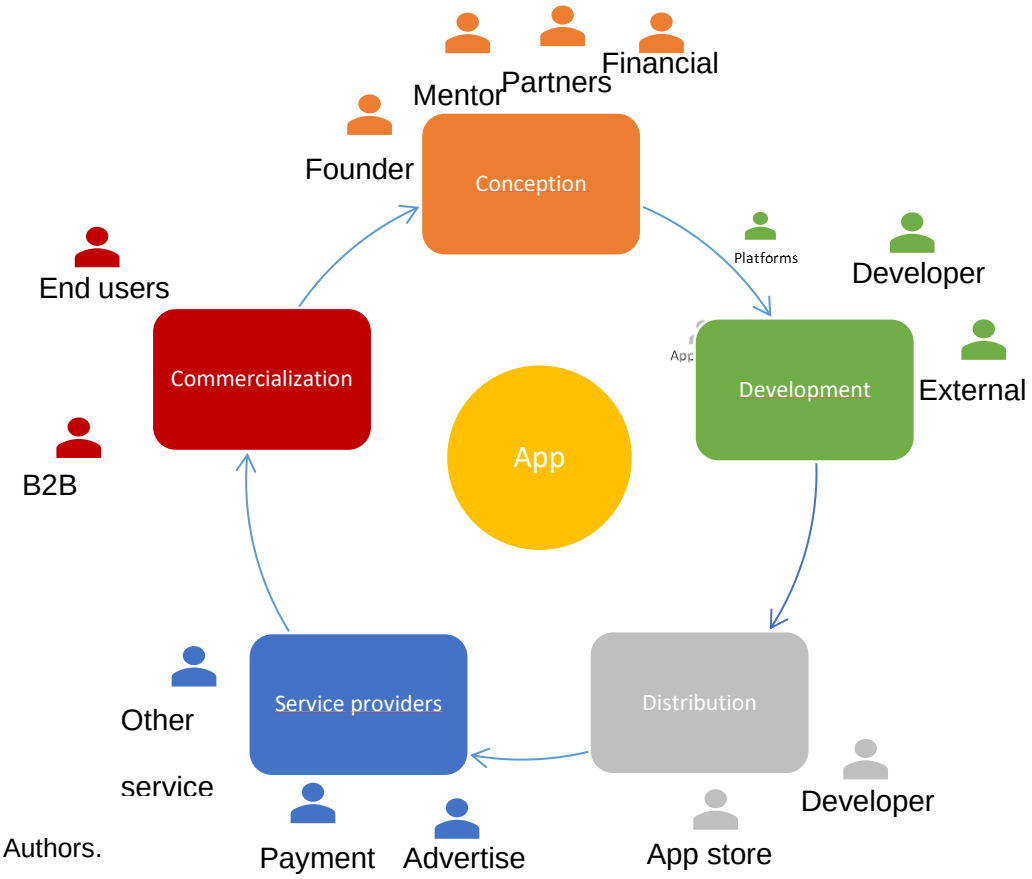
It provides stakeholders with the knowledge to consider and understand IP dispute resolution alternatives that align with their interests and to decide on appropriate strategies.

This chapter is divided into three sections:

1. **Court/judicial resolution**: reviewing the concepts of competent jurisdiction and choice of law, and the impact of mandatory law.
2. **Alternative dispute resolution**: looking at available alternatives to the courts and providing a description, pros and cons, concerns and grey areas of ADR, with references to the WIPO mediation and arbitration center and WIPO clause generator.
3. **Decision-making**: providing a practical view on how to decide between judicial resolution or ADR in the mobile app space.

Chapter 2 on the mobile app ecosystem presented several parties involved in mobile app development, distribution and commercialization (see Figure 6.1 below). These actors may have conflicting interests that give rise to disputes around the development, publication and commercialization of an app. IP-related disputes are of particular relevance, given they are costly for the parties involved, and can lead to drastic measures such as injunctions to prevent distribution of the app.

Figure 6.1 Key parties in app development, distribution and commercialization



Source: Authors.

6.2. IP-related disputes

Throughout the life cycle of a mobile app, from idea and conception and development through to distribution and commercialization, a multiplicity of conflicts can arise. Disputes may arise relating to different IP aspects of a mobile app, including ownership, control and/or commercialization rights, including copyright disputes about software code, patent disputes on inventions implemented in the app solution functionalities, trade secrets in algorithms, unauthorized use of content or license infringement.

Examples: potential disputes in relation to IP

- App owner and software development agency, regarding ownership, assignment and/or licensing of the mobile app software, or the quality or delivery of the mobile app.

- App owner and app store, regarding publication or removal of the mobile app from the store.
- End users and app owner, regarding conformity and quality of the mobile app, or damages caused by malfunction of the app.
- Third party and app owner, regarding compliance with the license on the third-party technology embedded in the mobile app.
- Third-party IP rights holder and app owner or end user, regarding breach of IP rights; for example, on content in the app, or a patented invention implemented in the app.

Moreover, as creating, exploiting and enforcing IP rights becomes more internationalized, in line with the globalization of technologies (especially mobile apps), companies and related industries, problems between stakeholders will probably transcend borders frequently and involve a complex mix of legal and technical issues. WIPO studies have demonstrated that disputes are more likely to arise when parties are based in different jurisdictions compared with a single jurisdiction,[25] just as a trend for collaboration between parties from different jurisdictions is being identified. In addition, during the commercialization stage, app owners may be faced with mandatory regulation, especially applicable to consumer end users, which creates a multiplicity of laws that may apply, depending on the user's domicile.

This situation leads to a complex scenario, and potential difficulty in determining the applicable legislation and the competent courts to deal with a dispute, as well as the diversity of applicable regulations. Parties may be forced into contentious proceedings with significant costs, long deadlines and unpredictable results. In this context, alternative dispute resolution mechanisms such as mediation, arbitration and expert opinion can be envisaged and provided for in agreements.

[25] World Intellectual Property Organization. Alternative Dispute Resolution Mechanisms for Business-to-Business Digital Copyright and Content-Related Disputes: Executive Summary. WIPO, 2021.

6.3. Judicial procedures

Traditional dispute resolution entails judicial procedures via civil courts. Filing a lawsuit in the competent court starts normal judicial proceedings, with the objective of having a judge hear and decide the case. This decision then must be enforced against the losing party. Local civil procedure legislation defines various stages of judicial procedures, often involving both written submissions and oral hearings, and possibly provisional measures, remedies and procedural actions. There are also rules as to which law should apply to the dispute, whether contractual or extracontractual (for example, tortious claims).

Choosing judicial procedure is, therefore, highly dependent on the legal system in which the claims must or may be brought, and which law applies.

6.3.1. Jurisdiction

The choice of court in the country to which the dispute should be brought is important for cross-border situations. When the parties come from different countries, the courts of both may be competent.

In business-to-consumer (B2C) relations, there are usually mandatory local laws that consider the consumer's domicile as the criteria to determine the competent court. For B2C mobile apps, this may put the app owner in one or many courts in several countries, which is generally not tenable for the business.

In business-to-business (B2B) situations, the agreement between the parties can usually set out which courts should be competent in the event of conflicts. In this respect, particularly between app owner and agencies (software agency developing the software), or between app owner and B2B clients, several factors should be considered when contractually agreeing on the competent courts, including:

- legal costs: consider the comparative costs of one court system over another (court fees, translation costs, attorney fees);

- legal interpretation: consider how courts have interpreted the most crucial aspects of the relationship, the agreement in question, and how that interpretation can affect each party (for example, available injunctions for copyright or patent infringement, or geoblocking).
- Judicial efficiency: delays or other deficiencies associated with a particular judicial system, such as difficulty of access or unfamiliarity with high technology agreements like those involved in the mobile app ecosystem.

Tip regarding judicial competence

While parties using standard terms often impose their own courts as competent courts for all claims (for more information on app stores terms and app users' EULAs, see Chapter 5), choosing the country of residence or establishing the defendant as the factor to determine the competence of courts, may limit the risks associated with the subsequent enforcement of a judgment.

In certain other situations, the competent court is set by law. For disputes over registration or the validity of registered IP rights such as patents, the courts of the State in which the IP rights have been registered have exclusive jurisdiction.

6.3.2. Choice of law

In relationships between parties in the same country (for example, the app owner and a local agency), the law of that country or territory will usually apply. For cross-border situations (for example, the availability of the mobile app in several countries or dealing with an app store in a different country), parties are advised to determine which law will be applicable in the event of a conflict over the relationship. There are several options, because, with the usual exception of consumer relationships, international treaties enable parties to agree on the applicable law:

- the law of the country of one or other of the parties;

- the law of the country where most activities under the contract are carried out;
- the law of a neutral country that has experience in the sector (brings equal costs and unfamiliarity with the system for both parties); or
- the law of the country of one or other against whom claims are being brought.

The underlying rule for IP disputes is that the law of the country where the IP rights arose applies to disputes regarding those rights.

Example: Choice of law China

Some countries have particular stipulations, including China, where it is mandatory to make domestic law applicable in disputes relating to IP rights protection in the country. Should a different law be chosen, the consequence may be that this clause, or the entire contract, will be declared void. Disputes on the performance and interpretation of the contract can, however, in general be governed by non-Chinese law.

Patent litigation

Patent litigation may occur in relation to apps. As was indicated in Chapter 4, the technology underlying mobile apps may be protected by patents, especially in the United States of America, where software patents have in the past been more commonly accepted by the US Patent and Trademark Office. There is a business model around patent infringement prosecution (otherwise known as Non Practising Entities (NPSEs) or "trolling") that moves a lot of money.

NPEs are popularly known as patent trolls, firms that do not produce goods and services from their patents but use them to sue other companies who do. In 2011, the estimated direct cost to defendants arising from NPE patent assertions was 29 billion US dollars.[a]

Patent infringement prosecutions are not just costly, with very long resolution times, but also complex. The underlying technology poses a challenge, and patent-inexperienced judges "often must devote an 'inordinate expenditure of time' simply to understand the technological jargon and rule on technological issues".[b]

Performing a freedom to operate analysis (known as "FTO") is the recommended action to reduce infringement scenarios. Further, Alternative Dispute Resolution (ADR)

appears to be a good way to avoid higher costs and time and provides a mechanism to agree on creative business-oriented solutions.

[a] Bessen, J. and M. J. Meurer. "The direct costs from NPE disputes." *Cornell Law Review* vol. 99, issue 2 (2014).

[b] United States Circuit Court. Parke-Davis&Co.v.H.K.Mulford Co. (two cases),189 F.95, 1911. https://case-law.vlex.com/vid/parke-davis-co-v-895252543

Case study: a dispute regarding mobile app technologies

In the United Kingdom, there was a dispute between an app owner and a technology provider (offering a software development kit or "SDK" for building apps) regarding the performance and functionality of the SDK technology. The app owner claimed the SDK provider was in breach of contract and stopped paying the fees, while the provider argued it had correctly delivered a fully functioning SDK and that it was the app owner who kept demanding more features and performance. Without an agreed solution, the dispute escalated. The technology provider terminated the license agreement contract, and sent taken down notices to app stores take down the app as it was now in breach of the license and further distribution infringed the provider's IP.

While standard judicial procedures were available, they were not sufficiently flexible and agile to offer a solution for the parties involved. ADR would have been a more appropriate decision to seek understanding and avoid significant legal costs and time.

Example: dispute-resolution clauses

Here we provide some example clauses that can be used to determine the dispute settlement procedure, jurisdiction and applicable law:

> "This Agreement shall be construed and interpreted by the laws of [choose the applicable law]. The court of [choose the jurisdiction to settle disputes] shall have jurisdiction."
>
> "This Agreement is governed by, and is to be construed in accordance with, [choose the applicable law]. The courts [choose the jurisdiction to settle disputes] will have nonexclusive jurisdiction to deal with any dispute which has arisen or may arise out of, or in connection with, this Agreement."

> "The Parties agree to submit all their disputes arising out of or in connection with this Agreement to the exclusive competence of the courts of [choose city (country)], and they waive any other jurisdiction to which they may be entitled."

6.3.3. Comment

Traditional dispute resolution mechanisms (that is, judicial resolution with its advantages and disadvantages), have been and are currently the standard for dispute resolution in the app space. The difficulty of effectively applying ADR mechanisms to disputes arising from tort liability (IP infringement), the complainant's search for procedures with an intimidating effect (and where publicity of decisions is vital), and, for consumer conflicts, the obligation mean to pursue redress is based on the consumer's domicile that judicial dispute resolution does not currently have, nor, at least to that extent, a competitive alternative. As for the preliminary measures that may be necessary to secure evidence or to stop the damage that IP infringement entails, arbitration injunctions have provided solutions, though limited only to those cases in which ADR has been agreed, again leaving aside noncontractual disputes.

Despite these scenarios, the ADR options analyzed below have the necessary potential and strength to become standard in the future.

More information is available on the WIPO website. For an update on the topics in this section, we refer the reader to the 2024 WIPO study on the localization of IP Infringements in the online environment, which, while focusing on the new technical scenario of the metaverse, is also relevant to the app space.[26]

6.4. Alternative dispute resolution

[26] World Intellectual Property Organization. "The Localization of IP Infringements in the Online Environment: From Web 2.0 to Web 3.0 and the Metaverse". *wipo.int*. 2024. <https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=622296>

As a response to the difficulties and limitations of traditional judicial dispute resolution, especially for cross-border transactions, ADR has grown and expanded globally.

The flexibility and the way ADR can be customized, and the strong role of party autonomy in procedures, can be attractive to parties in the mobile app sector looking to resolve disputes efficiently and effectively before a neutral party with the appropriate expertise.

In addition, the availability of ADR presents an opportunity to resolve disputes through less confrontational means, such as mediation, or to agree to resolve disputes via arbitration. Through ADR, parties can adopt simplified procedural rules and resolve multijurisdictional disputes in a single proceeding, resulting in time and cost savings, precious considering the short market cycles typical of apps. WIPO's experience suggests the use of ADR mechanisms includes more frequent settlement outcomes.[27]

The main disadvantage is that application must always be agreed between the parties since noncontractual breaches or damages such as IP infringement are rarely resolved automatically (or legal default) by such mechanisms. Also, when two parties are extremely uncooperative, nonbinding ADR may be used to stall and push the dispute out. Further, a court judgment will be preferable when, to clarify its rights, a party seeks to establish a public legal precedent rather than an award that is limited to the relationship between the parties.

In any event, it is important for actors in the mobile app sector and their advisers to be aware of their dispute resolution options to be able to choose the procedure that best fits their needs.

[27] WIPO Arbitration and Mediation Center. "Resolving IP and Technology Disputes through WIPO ADR" wipo.int March 2024. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_799_2016.pdf

6.4.1. Mediation

Mediation is a consensual process meant to solve disputes between parties, in which a neutral intermediary – the mediator – assists the parties in reaching a settlement, based on their respective interests. Characteristics include:

- **Informal**: the process is not marked by excessive rituals. It is not fixed and rigid but a relaxed process without many formalities. For example, WIPO mediation rules[28] impose on the claimant and respondent only certain minimum contents to be incorporated in their writing, such as "a brief statement of the nature of the dispute". And there are no strict deadlines defined a priori, with Article 13(a) stating: "As soon as possible after being appointed, the mediator shall, in consultation with the parties, establish a timetable for the submission by each party to the mediator."
- **Non-binding**: the mediator has no authority to issue any binding decision on the dispute unilaterally. The parties are not obliged to make a decision. If they wish to enter into a binding agreement, they may do so contractually through a settlement agreement; that is, with knowledge of the outcome of the mediation.
- **Role of the mediator**: The role may be said to be facilitative or evaluative

- in facilitative mediations, the mediator is less involved with the substance of the dispute and only facilitates the parties' discussions; and
- in evaluative mediations, the parties may request the mediator provide an assessment of the parties' respective positions.

- **Confidentiality**: information shared between parties that may be considered trade secrets, potential patents and others, are covered by the corresponding confidentiality agreement. This is a high point of mediation, as parties may share

[28] World Intellectual Property Organization. "WIPO Mediation Rules." *wipo.int*. 2021. <www.wipo.int/amc/en/mediation/rules>.

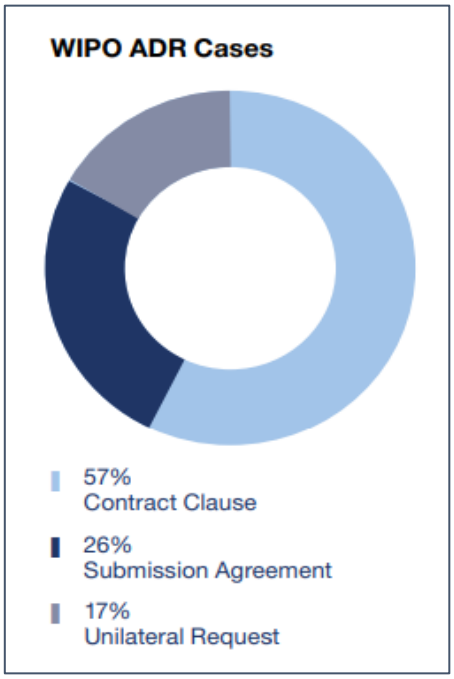
and discuss in a safe environment. In addition, the confidential nature of the process provides the parties with a platform to openly discuss the issues in dispute. A neutral mediator will be able to facilitate the airing of issues and assist in attempting to find a consensus based on the parties' respective interests, rather than solely by reference to strict legal rights.

- **Interest-based**: parties may consider non-legal factors such as business interests during negotiations, allowing them to preserve or develop their underlying business relationship.
- **Controlled by the parties**: either party may terminate the mediation at any time if it considers no progress is being made or the procedure is becoming too costly, or if the other party is not acting in good faith. This provides comfort to the parties involved.
- **Not final**: mediation leaves options open, such as litigation before the courts or arbitration.

There must be a mediation agreement between the parties, given this is primarily a consensual process, though there may also be court-mandated mediation in some jurisdictions as part of court proceedings. The mediation agreement may be previous to a conflict (for example, in a contract) or when a conflict arises. Parties refer disputes to mediation through:

- contract clauses;
- submission agreements; and
- unilateral requests.

Figure 6.2 WIPO ADR case breakdown



Source: World Intellectual Property Organization. Guide to WIPO Mediation. WIPO, 2018. <www.wipo.int/publications/en/details.jsp?id=4383>.

Example contract clauses

For WIPO mediation

Any dispute, controversy or claim arising under, out of or relating to this contract and any subsequent amendments of this contract, including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination, as well as noncontractual claims, shall be submitted to mediation in accordance with the WIPO Mediation Rules. The place of mediation shall be [specify place]. The language to be used in the mediation shall be [specify language].

Submission agreement:

We, the undersigned parties, hereby agree to submit to mediation in accordance with the WIPO Mediation Rules in the following dispute:

[Brief description of the dispute]

The place of mediation shall be [specify place]. The language to be used in the mediation shall be [specify language].

Unilateral request for mediation:

Article 4 of the WIPO Mediation Rules provides that a party may submit a written request for mediation to the WIPO Center and to the other party. In such event, the WIPO Center will assist the other party to consider the request for mediation and understand the mediation procedure.

Required content for the request:

- Parties:
  - identify the requesting party (name, country of domicile, contact data, representation data); and
  - identification of requested party (name, country of domicile, contact data, representation data).
- Dispute:
  - brief description of the dispute.
- Signature and submission to arbiter.mail@wipo.int and to the other party.

Source: World Intellectual Property Organization. "Request for WIPO Mediation." *wipo.int*. WIPO ADR. <www.wipo.int/amc/en/docs/request_mediation.docx>.

The WIPO Clause Generator[29] is a useful tool for drafting mediation and arbitration dispute resolution clauses.

Court referrals

In existing court proceedings, parties may have the opportunity to refer their dispute to WIPO mediation, either as suggested by the court or by agreement between them.

Outputs of mediation

Mediation may result in:

- **No agreement**: the parties do not come to any agreement. Under confidentiality obligations, mediation negotiations cannot be disclosed to third parties. Even in a subsequent judicial procedure, any statement made by the parties during a mediation process may not be disclosed. Mediation does not generally exclude

[29] The WIPO Clause Generator is online at https://amc.wipo.int/clause-generator/

the possibility of subsequent arbitration or litigation. Consequently, and to reinforce confidentiality, it is necessary to establish that the parties will not call the mediator to testify as an expert/witness in judicial proceedings related to the dispute. This is the object of the mediation and accordingly the mediator may waive their right to intervene as a witness or expert witness at the proposal/request of either party in any proceeding or litigation affecting the subject matter of the mediation.

- **Agreement achieved**: the parties reach settlement of their dispute. Mediation resolutions can be recorded as settlement agreements that have contractual force. If a party does not comply with the settlement agreement, the other party may rely on the courts to enforce it as a contract. The non-binding nature of mediation is modified by mutual agreement to become binding. International commercial settlement agreements resulting from mediation can be enforced in multiple jurisdictions under the United Nations Convention on International Settlement Agreements Resulting from Mediation (Singapore Convention on Mediation) of September 12, 2020, depending on whether a State is a signatory to the Convention. The enforceability of settlement agreements will be valuable to globalized businesses seeking consistent outcomes in multijurisdictional disputes.

Examples of domestic and regional ADR options

Philippines

The ADR of the Intellectual Property Office of the Philippines (IPOPHL) resolves IP disputes through mediation. The function is carried out by a dedicated unit, Alternative Dispute Resolution Services (ADRS), which is under the Bureau of Legal Affairs.

IPOPHL, in collaboration with WIPO, is also offering WIPO Mediation. This may be advantageous for international parties seeking resolution to related disputes in multiple jurisdictions. In existing court proceedings, parties may have the opportunity to refer

their dispute to WIPO Mediation, either as suggested by the court or by agreement between them.

Kenya

The Kenya Copyright Board (KECOBO) mediates copyright disputes in the audiovisual, publishing and music sectors. KECOBO is staffed by lawyers versed in mediating copyright disputes. KECOBO and the WIPO Center have teamed up to promote ADR and mediation for IP disputes in Kenya, providing parties with efficient and effective ways to resolve matters outside court. By working together, they provide a comprehensive and seamless ADR process, reducing the time, cost and stress of traditional court proceedings.

Trinidad and Tobago

In December 2018, the Intellectual Property Office of Trinidad and Tobago (TTIPO) and WIPO entered into a collaboration by signing a memorandum of understanding to make available ADR options, particularly mediation, for IP and technology disputes in the region through the WIPO Arbitration and Mediation Center (WIPO Center).

TTIPO offers a voluntary mediation option to parties to resolve pending trademark oppositions through mediation under WIPO Mediation rules.

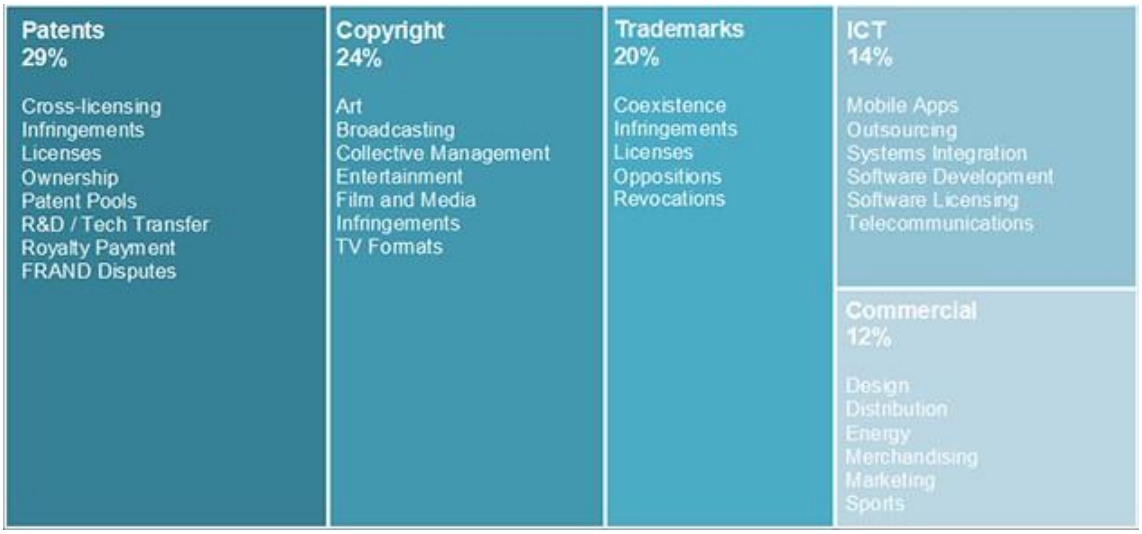
European Union

Online Dispute Resolution (ODR) is for out-of-court resolution of domestic and cross-border disputes concerning contractual obligations stemming from sales contracts or service contracts between a trader established in the European Union and a consumer resident in the European Union. This is through the intervention of an ADR entity that proposes or imposes a solution, or brings the parties together to help facilitate an amicable solution. The European Commission offers the freely accessible platform for out-of-court online dispute resolution, to which the parties can submit voluntarily, through the intervention of the Dispute Resolution Body that acts as an intermediary between the parties.

Figure 6.2 below shows the incidence of types of dispute in the total number brought to WIPO ADR for the period 2013–2023. They include not only IP disputes concerning patents, trademarks, information and communication technology (ICT), copyright and

entertainment, but also more general commercial matters such as marketing and distribution.

Figure 6.3 WIPO ADR case summary, 2013–2023



Source: World Intellectual Property Organization. "WIPO Caseload Summary." Web. Jan. 13, 2024. <www.wipo.int/amc/en/center/caseload.html>.

6.4.2. Arbitration

Arbitration is a process where parties agree to submit their dispute to be not just mediated but decided by a neutral party; that is, a tribunal consisting of one or more arbitrator(s) able to issue binding and final decisions known as awards.

Arbitration is increasingly being used by IP, technology, entertainment and other commercial stakeholders as a private procedure to resolve disputes involving such rights.[30] It is used particularly for domain name disputes, with WIPO one of the agreed arbitration centers providing this service for many top-level domains (TLDs).[31] While apps are usually distributed through app stores, there is frequently an associated website for promotion or even off-app sales or user registration.

[30] World Intellectual Property Organization: "Guide to WIPO Arbitration". Wipo.int. 2020 <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_919_2020.pdf>

[31] World Intellectual Property Organization. "Domain Name Dispute Resolution." *wipo.int*. visited March 2024. <www.wipo.int/amc/en/domains/>.

Characteristics include:

- **Formal**: arbitration is more formal compared with mediation, though not like a judicial procedure. It is still a private process but has formal rules, and the parties are bound by the arbitrator's decision. There are often established procedures and practices in place, ensuring the process follows a structured approach.
- **Consensual**: can only take place if both parties agree. Achieved by inclusion in their contract of an arbitration clause or, for existing disputes, conclusion of a submission agreement. In contrast to mediation, a party cannot withdraw from arbitration unilaterally.
- **Binding**: obligation to adopt and comply with the decision of the arbitrator. As in litigation (where the court typically has the power within its jurisdiction to issue a binding judgment), the arbitrator's role is to hear submissions from the parties according to agreed procedures and they may issue a final and binding award. If a party does not comply, the other party may still seek the court's assistance to enforce the arbitral award. It is possible to enforce arbitral awards in multiple jurisdictions under the 1958 Convention on the Recognition and Enforcement of Foreign Arbitral Awards, or New York Convention (see chapter 8).[32] Such international enforceability will be valuable to globalized app businesses seeking consistent outcomes in cross-border disputes.
- **Interim relief**: in arbitration, the arbitral tribunal is usually empowered to grant interim orders. Interim relief may be required for a variety of reasons, including to preserve evidence or protect assets. In app-related disputes involving breach of IP licenses, an interim injunction may be sought pending resolution of the dispute, to prevent further unauthorized use of the IP by the party in breach, especially when the IP involves proprietary information or trade secrets.

---

[32] World Intellectual Property Organization. "Convention on the Recognition and Enforcement of Foreign Arbitral Awards." *wipo.int*. Jun. 10, 1958. <www.wipo.int/amc/es/arbitration/ny-convention/>.

- **Confidential**: considerations regarding confidentiality for mediation presented in section 6.4.1 above also apply to arbitration, though in arbitration confidentiality extends to the possible award.
- **Award**: the decision of the arbitral tribunal is final and easy to enforce. It is possible to enforce arbitral awards in multiple jurisdictions under the New York Convention, and, again, will be valuable to global app businesses.

During the proceedings, the arbitral tribunal will hear submissions from the parties according to agreed procedures. Significantly, arbitration procedures can be more flexible compared with civil procedure requirements in court litigation, and parties have the autonomy to decide on various aspects, including the composition of the tribunal, procedural rules that should apply and geographical location of the arbitration.

Examples of arbitration laws

Kenya

In Kenya, Arbitration Act, No. 4 of 1995 (the Act) provides for forms of an arbitration agreement. The courts have generally enforced arbitration agreements except in instances where they fall within the exceptions provided in Section 6 of the Act; that is, where the court finds that the agreement is null and void, inoperative, incapable of being performed or that there is in fact no dispute between the parties about the matters being referred to arbitration.

Philippines

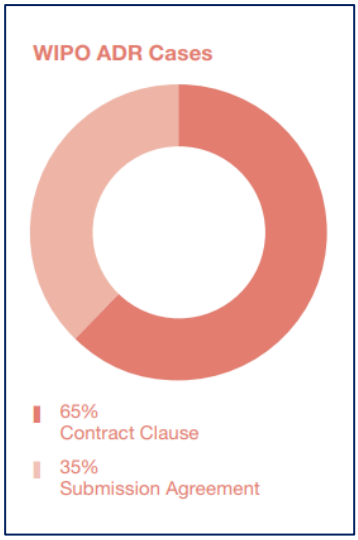
Rules promulgated pursuant to Republic Act No. 9285 (Alternative Dispute Resolution Act of 2004, or ADR Law) resolve a dispute by rendering an award. Under the law, international commercial arbitration is governed primarily by the United Nations Commission on International Trade Law (UNCITRAL) Model Law 1985, and domestic arbitration by Republic Act No. 876 enacted in 1953 (Arbitration Law).

When to decide on arbitration?

The arbitration agreement may be used for disputes that have arisen or which may arise. Parties refer disputes to arbitration through:

- Contract clause.
- Submission agreement.

Figure 6.4 WIPO's Alternative Dispute Resolution Cases, 2020



Source: World Intellectual Property Organization. Guide to WIPO Arbitration. WIPO, 2020.

Submission to WIPO arbitration

Sample contract clause

Any dispute, controversy or claim arising under, out of or relating to this contract and any subsequent amendments of this contract, including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination, as well as noncontractual claims, shall be referred to and finally determined by arbitration in accordance with the WIPO Arbitration rules. The arbitral tribunal shall consist of [a sole arbitrator][three arbitrators]. The place of arbitration shall be [specify place]. The language to be used in the arbitral proceedings shall be [specify language]. The dispute, controversy or claim shall be decided in accordance with the law of [specify jurisdiction].

Submission agreement:

We, the undersigned parties, hereby agree that the following dispute shall be referred to and finally determined by arbitration in accordance with the WIPO Arbitration rules:

[brief description of the dispute]

The arbitral tribunal shall consist of [sole arbitrator][three arbitrators]. The place of arbitration shall be [specify place]. The language to be used in the arbitral proceedings shall be [specify language]. The dispute shall be decided in accordance with the law of [specify jurisdiction].

The WIPO Clause Generator[33] is a useful tool for drafting arbitration dispute resolution clauses.

Outputs of arbitration

Arbitration can result in:

1. Agreement achieved through arbitration: before the award, the parties can record a settlement agreement that has contractual force. If a party does not comply, the other party may rely on the courts to enforce the agreement as a contract. International commercial settlement agreements resulting from arbitration have had the possibility of being enforced in multiple jurisdictions since September 12, 2020, under the United Nations Convention on International Settlement Agreements Resulting from Mediation (Singapore Convention), depending on whether a State is signatory to the Convention.
2. Award: the decision of the arbitral tribunal is final and easy to enforce. As a private alternative, arbitration normally forecloses court options. Most arbitration awards are voluntarily complied with without the award creditor having to initiate recognition and enforcement proceedings. This may be as much a reflection of the powerful enforcement mechanism provided by the New York Convention as it is a sign of acceptance of the legitimacy of the arbitration process.

[33] The WIPO Clause Generator is online at https://amc.wipo.int/clause-generator/

WIPO Arbitration Rules

Article 66 of WIPO Arbitration Rules implies a waiver by a party of any "right to any form of appeal or recourse to a court of law or other judicial authority", to the extent that such a waiver may be made under the applicable law.

The applicable law in relation to recourse against an arbitral award is the law of the place of arbitration. This is the *lex arbitri* (or law of the arbitration) that determines the extent of available recourse against an arbitration award. Almost invariably, that recourse is before the courts of the place of arbitration.

The principal question arising from Article 66 is whether the waiver language would suffice to remove recourse against an arbitration award in places such as Switzerland, where in certain circumstances it is permitted for parties to waive all recourse against an award, even where it is contrary to public policy. Thus, in Switzerland, this would almost definitely not suffice.[a]

[a] Phillip Landolt and Alejandro García: "Commentary on WIPO Arbitration Rules". wipo.int. 2017 < https://www.wipo.int/export/sites/www/amc/en/docs/2017commentrulesarb.pdf>

6.4.3. Expedited arbitration

Given the need for rapid resolution, especially in technology cases or those not highly complex, expedited arbitration appears a valid option. The intervention of a single arbitrator and reduced time and costs are a move in the desired direction. The main ADR institutions, such as the WIPO Center, have fast-track arbitration rules to facilitate such procedures. Furthermore, a mediation settlement may also include creative business-oriented solutions.

For more information, see the WIPO comparison chart, which is summarized in Table 6.6 below.

Table 6.1 Mediation vs. arbitration

	Mediation	**Arbitration**
Cost	Generally, mediation is a more cost-effective method of dispute resolution than arbitration, as the process can be completed in a shorter time frame.	
Party autonomy and control	Parties are in control over the negotiations and outcome of the proceedings. Allows parties to preserve or develop their underlying business relationship.	Focused on the legal issues in dispute and may not consider the business interests of the parties in the way that is possible with mediation.
Subject matter	Enables parties to consider non-legal factors such as the business interests of the parties during negotiations.	Focused on the legal issues in dispute.
Style	Less adversarial. Enables parties to maintain amicable relationships. The possibility of continued collaboration post-mediation is a genuine prospect and should be considered by parties who seek to maintain business relationships. Mediation settlement may also include creative business-oriented solutions.	Somewhat more adversarial.
Facts	Parties are often encouraged to establish agreed factual positions, and this may result in issues in dispute being more clearly identified.	Greater uncertainty as to the potential determinations as to findings of fact, especially when the credibility of witnesses is at issue or if there is uncertainty on a point of law
Right to withdraw	A party may decide to unilaterally terminate the mediation for various reasons; e.g. where the mediation seems ineffective or the process is not cost-effective.	Parties are usually not permitted to withdraw from arbitration unilaterally once it has been commenced. If a party fails to attend arbitration proceedings, the arbitral tribunal may issue a default award.

Source: Authors.

Mediation case examples

Software license dispute

A European software developer entered into a software licensing agreement with a European customer that included a contract clause providing for WIPO Mediation followed by court litigation.

In a dispute regarding non-execution of the agreement and related damages claims, the parties initiated mediation and the WIPO Center appointed a mediator with experience in technology contracts. The mediation sessions took place online, with live interpretation, and a settlement agreement was concluded within six months of the commencement of the mediation.[a]

Trademark dispute

After a dispute arose between them, a North American company requested mediation with two Italian companies and one Spanish company on the basis of an agreement that the parties had reached under WIPO Mediation Rules. The aim was to help the parties avoid confusion and misappropriation of their similar trademarks and regulate their future use.

Two months later, the mediator met with the parties in a two-day session in Milan. The meeting was held in joint session except for two brief caucuses. At the end of the second day, the parties – with the mediator's assistance – were able to draft and sign a settlement agreement covering all pending issues in dispute.

Source: World Intellectual Property Organization. "WIPO Mediation Case Examples." *wipo.int*. Web. Jan. 14, 2024. <www.wipo.int/amc/en/mediation/case-example.html>.

6.4.4. Mixed solutions, reliance on mediation and arbitration

While mediation and arbitration are distinct dispute resolution procedures, mediation may also be used in conjunction with arbitration to enable parties to resolve disputes more effectively. In the past five years, parties have made use of innovative ADR processes such as sequential mediation-arbitration (Med-Arb) escalation procedures. Additionally, parties may start mediation during arbitral proceedings.

1) Med-Arb

In a typical Med-Arb arrangement, parties first submit the dispute to mediation to explore any possibility of settlement, and second, if no settlement is reached, the dispute is submitted to arbitration. Advantages include:

- Med-Arb provides effective resolution of disputes between the parties.
- Even if parties fail to reach a settlement during mediation, the process is valuable, given it may assist in narrowing the issues in dispute, allowing for a quicker resolution in subsequent arbitral proceedings.
- The parties may also agree on procedural or substantive points, which may allow them to focus the arbitration proceedings on particular issues. For example, the parties may, during mediation sessions, agree a method of computing damages to be adopted by the arbitral tribunal.

In some instances, the mediator also acts as the arbitrator in subsequent arbitral proceedings. This may be advantageous, as the arbitrator will be familiar with the dispute and arbitration may be conducted more efficiently. It may, however, raise practical problems, such as parties being less likely to negotiate openly.

WIPO Med-Arb

More information on the WIPO Med-Arb clause is available on the WIPO website, www.wipo.int/amc/en/clauses/med_arb/.

2) Mediation during arbitration

During the arbitration process, the parties may also commence mediation, either at the suggestion of the arbitral tribunal or of their own accord. The mediation process may be concurrent or may take place while arbitration is suspended.

As ADR procedures are not generally mutually exclusive, the parties to an app-related dispute are usually free to customize the dispute resolution process to best meet their

respective commercial interests, such as time and cost efficiencies, or preservation of amicable business relations. ADR procedures may be combined strategically to resolve disputes effectively, and to help parties resolve their disputes in a manner that maximizes the opportunities for maintaining their relationship.

Example of mediation during arbitration

In a dispute between a software company and a publishing house on the development of a new web presence, the publishing house was dissatisfied with the deliverables and refused to make payments. The parties initiated mediation before proceeding to expedited arbitration at the WIPO Center. During the arbitral hearing, the parties indicated a willingness to settle the dispute and sought a settlement proposal from the arbitrator, which was accepted by the parties and subsequently recorded as a consent award.

6.4.5. Expert determination

Expert determination is a procedure where a situation or a dispute is submitted, by agreement of the parties, to one or more experts who make a determination. This is particularly useful in highly complex technical situations or where an objective opinion (such as IP valuation or calculating royalties on patented technologies) is sought without going to dispute resolution.

Characteristics:

- **Consensual**: expert determination can only take place if both parties agree to it. With future disputes/differences arising under a contract, the parties insert an expert determination clause in the relevant contract. An existing dispute/difference can be referred to expert determination by means of a submission agreement between the parties. The expert determination agreement will usually contain the procedure for the expert determination, although parties may also decide to rely on institutional rules. In contrast to mediation, a party cannot unilaterally withdraw from arbitration.

- **Neutral and flexible**: in addition to selecting an appropriate expert, the parties are able to choose important elements such as the language of the expert determination or the place of any meeting. When seeking a quick determination on a straightforward matter or specific issue, it can be less structured than arbitration and litigation.
- **Confidential**: information shared between parties that may be considered trade secrets, potential patents and others, are covered by the corresponding NDA. This is meant for their comfort, enabling them to share and discuss in a safe environment, and to protect the confidentiality of the expert's determination, any disclosures and the resulting determination.
- **Binding**: in principle, the determination of an expert is binding, with contractual effect between the parties. Alternatively, by party agreement, the determination may have effect as a recommendation to the parties. In this scenario, it may still be useful, as parties may rely on it in subsequent negotiations/mediation or as evidence in arbitration or litigation proceedings, subject to the applicable rules of evidence and procedure governing the proceedings.
- **Parties choose experts with relevant expertise**: in a contractual submission, or under the WIPO Rules, the parties can select an expert together. If the parties have not agreed on the expert, or on a different procedure for appointing the expert, the expert will be appointed by a third party such as the WIPO Center after consultation with the parties. The center has access to experts with specialized knowledge relevant to IP issues in a broad range of technical and business areas, which allows it to propose and appoint the appropriate experts.

6.4.6. Multitiered or escalation ADR mechanisms

It is also possible for parties to agree on multitiered processes to resolve disputes. This will typically involve parties layering ADR procedures by way of an escalation clause; for example, mediation followed by arbitration (or expedited arbitration) if a settlement is not

reached during mediation. Such clauses may facilitate settlement while allowing parties the freedom to escalate at any stage.

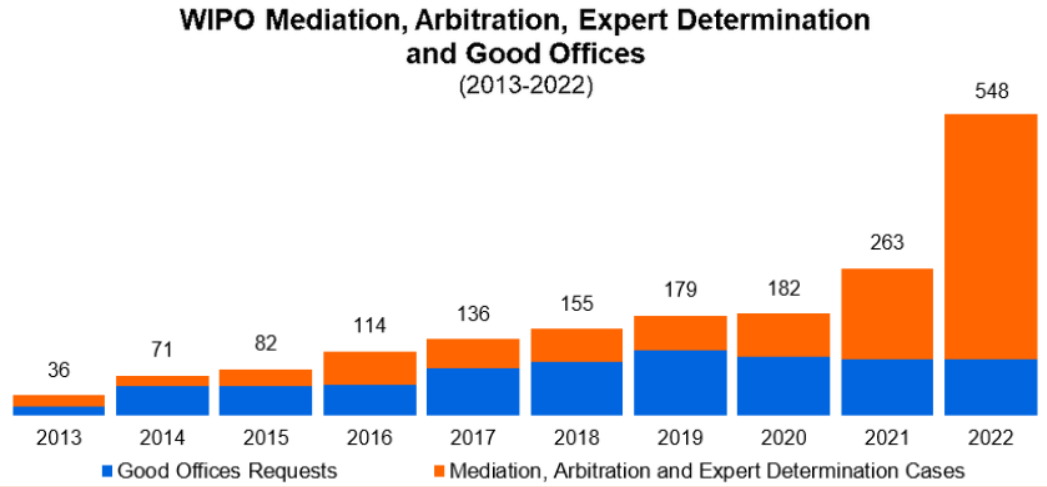
The way ADR can be customized features strongly in multitiered procedures. For instance, depending on the agreement between the parties, the same person may be chosen as the mediator and the arbitrator if the dispute is escalated. This may be advantageous, because the arbitrator will already be familiar with the dispute, with potential cost savings.

WIPO multitiered processes

More information on WIPO multitiered processes is available on the WIPO website, www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo_mobile_apps_disputes_guide.pdf.

WIPO mediation, arbitration, expert determination and good offices (2013-2022)

In 2022, the WIPO Arbitration and Mediation Center experienced a 105 per cent increase in the IP ADR caseload. In total, it received 548 mediation, arbitration, expedited arbitration cases and good offices requests.



Particular increases in requests for mediation came in copyright disputes (especially through coadministration collaboration with the national copyright offices of Colombia and Mexico), FRAND-related disputes and international IP disputes referred by Chinese courts. Other observations included:

- Disputes involved a broad range of IP areas, with copyright (72 per cent), trademarks (12 per cent) and patents (8 per cent) most common.
- WIPO cases involved SMEs, including start-ups, creators and innovators (46 per cent), collective management organizations (22 per cent), multinationals (16 per cent) and other entities, including universities and research and development (R&D) centers (16 per cent), with parties coming from all regions, notably Asia, Europe, Latin America and North America.
- The main business sectors in cases were creative industries, ICT, life sciences and mechanical processes/equipment.
- Procedures were conducted in multiple languages, including Chinese, English, French, Korean and Spanish.

In most cases, parties used WIPO Online Case Administration Tools, including the WIPO Center's eADR online case management platform and videoconferencing systems. The necessary use of online tools occasioned by COVID-19 pandemic restrictions in 2020 and 2021 continued through 2022

6.5. ADR enforcement

A party that has successfully litigated before the courts may seek enforcement of the judgment in a foreign jurisdiction. Enforcing foreign judgments in most jurisdictions usually involves a degree of procedural complexity, however, and courts may apply different rules on recognizing the judgment; for example, in jurisdictions where courts are obliged to review the merits of a foreign judgment relating to IP disputes, it is unlikely the judgment will be enforced.

Arbitral awards and mediation agreements may be enforceable internationally with greater certainty.

As of August 2023, 172 states (including Kenya, Philippines and Trinidad and Tobago) recognized and enforced international arbitral awards under the New York Convention.[34] The convention generally requires contracting States to enforce an arbitral award

[34] "The New York Convention." *newyorkconvention.org*. <www.newyorkconvention.org/>.

rendered in another state that is also a party to the convention if the dispute is of a commercial nature.

With international mediation agreements, European Directive 2008/52/EC (Mediation Directive) on aspects of mediation in civil and commercial matters imposes an obligation on Member States to ensure the enforceability of certain cross-border mediation agreements.

In addition, the Singapore Convention requires contracting parties to enforce international mediation agreements.

6.6. Decision-making: what to do

While judicial procedure is still the default for dispute resolution, including in the app sector, as discussed, ADR appears to be a valid alternative. This section attempts to provide a practical view on how to decide between judicial procedure or ADR in the mobile app space.

Table 6.7 presents the main differences and use cases to which the different resolution mechanisms are best suited.

Table 6.2 Comparison on ADR and judicial procedures

	ADR	Judicial
Costs	Often avoids unforeseeable costs. Predefined costs and timings.	Entails higher costs, including attorney fees, court costs and expenses for witnesses. Parties should determine who pays these costs (i.e., losing party).
Jurisdictions	Single forum. Parties may resolve multijurisdictional disputes in a single action.	Multiple jurisdictions with the risk of a multiplicity of inconsistent outcomes. This needs to be considered, as some jurisdictions may benefit each party. Protecting IP rights may not be identical across jurisdictions, with the possibility of a diversity of outcomes

		where a party succeeds in one jurisdiction but fails in another.
For app owners, given apps are commercialized on an international scale, litigation will probably be multijurisdictional. If the app incorporates third-party IP, the app owner will need to obtain licenses to use such IP in multiple jurisdictions in relation to each relevant area of use. Litigation may arise in relation to the various licenses.		
Party autonomy	Parties have the autonomy to shape the ADR proceedings to best fit the context of their disputes and commercial requirements.	Parties are bound by the applicable civil procedure rules of the national courts. Provides legal certainty.
Expertise of the neutral	Parties in ADR may select an appropriate neutral with a particular expertise, which can contribute significantly to achieving quality outcomes in highly technical app disputes. A suitably proficient neutral may also lend greater efficiency in the conduct of the proceedings.	There is a lower learning curve relative to judges in litigation (who may not always have the specific technical proficiency in the relevant area). This may translate into added time and cost.
Procedural flexibility	Parties can either devise their own rules to govern the ADR proceedings, adopt UNICTRAL Arbitration Rules, or more commonly, opt for the rules of leading ADR institutions (i.e., institutional rules). Parties further tailor the rules to suit their needs by specifying - time-limited procedures for the appointment of the arbitral tribunal; - the expertise of persons appointed to sit on the arbitral tribunal; - the scope of evidence that may be admissible; and	Rigid and predefined. Provides legal certainty.

	- the deadlines for the hearing and delivering of the arbitral award. This enabled arbitration of a dispute to be completed within just three months after filing the request. (expedited arbitration example).	
For app owners, where the average product life cycle of an app is generally shorter than that of products in other industries, quick resolution of disputes is of great value to parties.		
Confidentiality	Allows for confidentiality of proceedings and decisions.	More difficult to achieve confidentiality.
Remedies	Parties not necessarily bound by the limitations of the courts in respect of remedies. ADR may lead to outcomes that are sensitive to the commercial interests of the parties.	Normally restricted by prescriptive statutory instruments in litigation.
In the mediation process, the informal nature of the proceedings allows parties to negotiate creative business-oriented solutions that can be broader than remedies provided under the law and more aligned with their respective interests. Such solutions may be recorded in a settlement agreement between the parties and enforced as a binding contract.		
Elapsed time	ADR allows short time frames that parties may further customize, and bespoke procedures that consider the commercial requirements of the parties. These can provide significant cost savings.	Considerably longer time frames. Related to previous considerations.
Finality	Arbitral awards are not normally subject to appeal (see section Outputs of arbitration).	Court decision can generally be contested through one or more rounds of litigation.
Enforceability	The New York Convention generally provides for the recognition of arbitral awards on par with domestic court judgments without review on the merits.	The recognition and enforcement of foreign judgments in most jurisdictions usually involves a degree of procedural complexity.
Applicable to third parties	No. ADR is limited to the relationship between the parties.	Not directly. But will be considered as a precedent for future decisions.

Deterrent to third parties	No. It is confidential	Yes (e.g., patent infringement)

Source: Authors.

6.7. Conclusions

According to Statista data, the apps market is expected to reach 673 billion US dollars by 2027, compared with 522 billion US dollars forecast for 2024. This implies an annual growth rate (CAGR 2022–2027) of 8.58 per cent.[35] This growth suggests that cross-border disputes will continue to grow in parallel and that dealing with them will require huge investment.

Besides, some disputes are likely to remain unsuitable for resolution by ADR; for example, in cases where the alleged wrongdoer is unlikely to agree to submit to ADR, or in relation to end user-related app disputes where national consumer protection laws may restrict the use of ADR mechanisms.

Better ADR understanding and strong divulgation will continue to be the key to success, to the benefit of the whole app ecosystem. Players must understand the potential of ADR to achieve objectives and allocate resources more efficiently.

Key takeaways

- Diverging interests among actors within the mobile app sector means there may be conflicts between them.
- These conflicts often evolve around IP, licensing and compliance.
- There are traditional judicial dispute resolution procedures and alternative non-judicial procedures (ADR) such as mediation or arbitration. Both have pros and cons.
- Parties to an agreement should carefully consider whether they want to submit any future dispute to the courts or an ADR mechanism.

[35] Statista. "App – Worldwide." *statista.com.* Web. Jan. 14, 2024. <www.statista.com/outlook/amo/app/worldwide>.

- WIPO offers an ADR Center for dealing with IP-related disputes, and suggests the appropriate wording for incorporating submission to this mechanism in contractual documents.

6.8. Useful links and resources

WIPO, *Intellectual Property Toolbox For Mobile Applications Developers.* < https://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo_ip_toolbox_mobile_apps.pdf>

WIPO, *Guide on Alternative Dispute Resolution for Mobile Application Disputes*. http://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo_mobile_apps_disputes_guide.pdf

WIPO, *Alternative Dispute Resolution*.< http://www.wipo.int/amc/en/>

WIPO, *Guide to WIPO mediation.* 2020 < *https://tind.wipo.int/record/29081?v=pdf*>

WIPO, *Guide to WIPO Arbitration. 2020* < https://tind.wipo.int/record/42701?v=pdf>

WIPO, *Alternative Dispute Resolution Mechanisms for Business-to-Business Digital Copyright and Content-Related Disputes*. 2021 <http://www.wipo.int/edocs/pubdocs/en/wipo-pub-969-en-alternative-dispute-resolution-mechanisms-for-business-to-business-digital-copyright-and-content-related-disputes.pdf>

WIPO, *Results of the WIPO Arbitration and Mediation Center International Survey on Dispute Resolution in Technology Transactions*. 2013 http://www.wipo.int/export/sites/www/amc/en/docs/surveyresults.pdf

IPOHL IP Mediation < https://www.ipophil.gov.ph/ip-mediation/> and *WIPO Mediation Proceedings Instituted in the Intellectual Property Office of the Philippines* (IPOPHL) Visited March 2024 http://www.wipo.int/amc/en/center/specific-sectors/ipophl/

WIPO, Intellectual Property and the Judiciary. 2018 https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_13/wipo_ace_13_8_ppt.pdf>

WIPO, The Localization of IP Infringements in the Online Environment: From Web 2.0 to Web 3.0 and the Metaverse. September 2023 https://www.wipo.int/export/sites/www/respect-for-ip/en/docs/case-strudy-the-localiaztion-of-ip-infringement.pdf.

Chapter 7. Financing and commercialization of IP in mobile apps

7.1. Introduction

The purpose of this chapter is to look at the financial aspects of mobile apps, particularly those relating to IP, to enable app owners to identify an appropriate strategy based on the nature of the mobile app and its business model, secure funding through its IP, and choose the most appropriate way to commercialize the app.

The critical role that IP plays in the financial and commercial value of a mobile app is highlighted, and the strategies to monetize app-related IP such as patents, trademarks and copyrights, through licensing or direct sales, are detailed. The chapter discusses how well-managed IP can attract investors, increase market value and provide competitive advantages. It also underscores the importance of IP protection to prevent reduced value due to unauthorized use and ensure profitability and presents IP as an integral part of a successful mobile app financing and commercialization strategy.

This chapter is divided into two sections. The first addresses how a mobile app can be financed through internal funding (not affordable for everyone) and external funding (not easy for SMEs that lack a large portfolio of tangible and intangible assets to offer as security). The main problems for an SME in securing financing are considered, as well as how IP management can help overcome these problems; for example, by creating a strategy that allows the app owner to identify, protect and exploit IP and create an IP portfolio to make it more attractive for securing external financing.

Th second section explores the different avenues for commercializing the IP of a mobile app and the types of relationships that the main stakeholders might establish to support these efforts. There are various ways to commercialize mobile apps, taking account of their business models. The types of relationships that can play a significant role in the

commercialization process are examined, including commercialization by the IP owner, licensing, assignment and partnerships or joint ventures.

More information on these topics is available in the 2021 WIPO paper, *The role of IP rights in the development and commercialization of mobile applications*.[36]

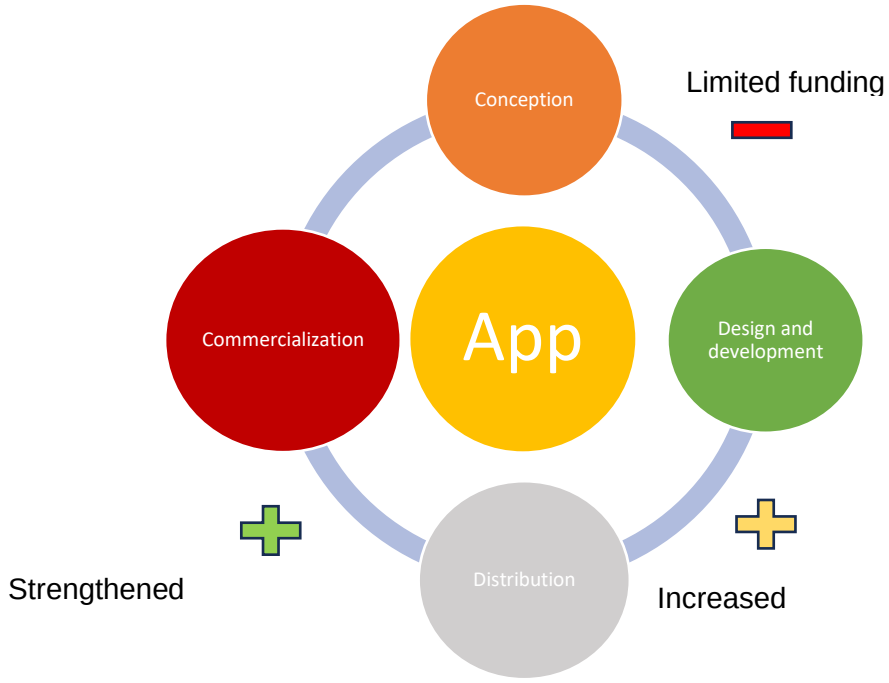
7.2. Mobile app financing through IP

7.2.1. Introduction

In the mobile app industry, IP can be an asset for leveraging financing and thus worth considering in the financing strategy. Intangible assets behind the mobile app may be more valuable, in financial terms, than the app itself. There are various forms of IP that can exist in a mobile app (see chapter 4). While there are several business models that app owners can opt for once they launch the app (see chapter 3), before reaching this launch stage they may encounter difficulties in securing funding to launch the app and commercialize it. IP protection and optimization is one way to overcome this.

[36] WIPO. The role of IP rights in the development and commercialization of mobile applications. 2021 < http://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo_iprs_mobile_apps.pdf>

Figure 7.1 Securing funding at different phases of mobile apps life cycle



Source: the authors.

Funding opportunities may increase as the development process progresses:

- At the concept stage, when the app is just an idea, the likelihood of funding options is lower than when it develops into a minimum viable product (MVP) or prototype, though it is possible to demo the app to investors.
- At later stages, after proof of concept or prototyping, it may be easier to obtain financing with a demonstrable technology. From an IP perspective, there are more assets to protect and exploit.
- After launch, the app may be producing income, an easier basis for financial valuation and obtaining financial support.

Notwithstanding the chances of financing at different stages of the app's life cycle, app owners should be aware of the need to identify the IP that may be generated in each of the stages, to protect and defend its value. Thus the IP is configured as an essential

instrument to ensure the financing of the app and guarantee its launch and positioning in the market.

The following section will present the key steps that will help individual app owners or agencies developing software for apps (if applicable) identify the IP generated in the app life cycle and give it a value in order to position it in the corresponding market and secure funding.

7.2.2. IP strategy

During the ideation process, entrepreneurs brainstorm and conceive novel ideas that could revolutionize the mobile app market. These ideas, which serve as the bedrock of any successful mobile app, are intangible assets that can be easily replicated or imitated if not guarded. It is imperative, therefore, that businesses recognize the value of these innovative concepts from the outset.

As the ideation transitions to the product/service development phase, the IP strategy becomes even more crucial. This is the stage where the abstract concepts begin to take shape, and technologies, codes and unique user interfaces are developed. Without a comprehensive IP strategy, there is a heightened risk of such innovations being copied or modified by competitors, leading to potential revenue loss and dilution of market positioning. Safeguarding the proprietary features and functionalities of the mobile app through patents, copyrights or trademarks during this phase ensures the app owner's hard work and investment are not easily undermined.

Finally, IP protection and commercialization go hand in hand. Once IP rights are secured, the app owner can confidently explore various avenues to monetize its assets. This can range from licensing the technology and IP to third parties, to establishing partnerships or directly generating revenue through user subscriptions or in-app purchases. Moreover, a robust IP portfolio serves as an attractive asset in mergers and acquisitions or when seeking investment. In essence, an effective IP strategy not only offers legal

protection but also opens diverse channels of revenue generation, making it indispensable in the competitive landscape of the mobile app sector.

The key IP issues to consider at the different stages of the app life cycle are indicated below.

Table 7.1 IP strategy issues to consider at different stages of the app life cycle

Stage 1	**Ideation process**
Commercial application	Does the idea/concept have commercial application?
Identifying IP assets	Does the business have processes and/or procedures for identifying IP assets within the business?
Capturing IP assets	Does the business have processes and/or procedures for capturing IP assets?
Confidential information	Does the business have processes and/or procedures for preventing disclosure of the idea/concept (NDAs, trade secrets, restricted access, other agreements)?
Likelihood of IP protection	Does the business have processes and/or procedures to identify the likelihood of obtaining IP protection (preliminary patent, design, trademark, copyright, domain name, plant breeder's rights searches)?
Partnerships	Does the business have potential partners for collaboration in developing and commercializing the idea/concept? When collaborating with third parties, will the business secure ownership or access to the IP?
Identifying competitors	Does the business have processes and/or procedures to identify competitors or the likelihood of infringing third-party rights by applying the idea/concept?

Stage 2	**Product / service development**
Freedom to operate search	Does the business conduct IP landscape, freedom to operate (FTO) searches or competitor analysis to identify any potential competing IP rights or technologies?

IP searches	Does the business conduct regular IP and technology searches to determine the likelihood of obtaining IP protection for the incremental innovations or improvements?
Third-party rights	Does the business have processes and/or procedures for addressing IP ownership considerations when collaborating with third parties to develop its product and services (marketing, employer, R&D, licensing agreements)? When collaborating with third parties, has the business secured the rights to use the results of the IP developed during the collaboration? Does the business use the IP of third parties? If so, has the business acquired the rights to use the IP?
IP strategy implementation	Does the business have a technical or IP review committee to decide on product or service development, considering the overall business and IP strategy?

Stage 3	**IP protection**
IP protection strategy	Has the right protection strategy been identified (i.e., patent, trade secret, design, trademark, open source, plant breeder's rights, copyright IP)?
Prioritization of IP protection	Does the business have processes and/or procedures for prioritizing IP protection (i.e., the order in which IP rights and protection are prioritized)?
Technology landscaping	Does the business conduct IP searches and/or technology landscape studies for patent, design, trademark or plant breeder's rights before seeking protection?
IP strategy development	Does the business have processes and/or procedures for developing an IP strategy, including market, cost or timing considerations?
Monitoring ownership	Does the business have processes and/or procedures for monitoring inventorship, authorship and ownership considerations?
Non-registerable IP protection	Does the business have processes and/or procedures for protecting non-registerable forms of IP know-how, trade secrets, goodwill, etc.
IP advice	Is advice sought from IP professionals before pursuing IP protection?

IP strategy alignment	Is the IP strategy aligned with the commercialization strategy?

Stage 4	**IP commercialization**
Commercialization vehicle	Does the business have processes and/or procedures to identify the appropriate commercialization vehicle (manufacture, sale, license, etc.)?
IP asset valuation	Does the business have processes and/or procedures for the of valuation of IP assets, especially for those to be licensed as part of business model/pricing strategy for products (e.g., claim charting vis-à-vis competitor products/services)?
Freedom to operate	Has a freedom-to-operate search been conducted to determine the potential to infringe third-party rights?
Competition monitoring	Does the business have processes and/or procedures for monitoring competitor activities, potential commercialization partners or enforcement of IP rights?
Branding	Is the product and/or service appropriately branded (trademark, packaging, websites, domain names)? Is descriptive or distinctive branding considered?
IP review	Does the business have an IP and innovation review board within the business to periodically review IP assets, portfolio structure, new innovations and disclosures, competitive landscape, IP budget, etc.?
IP audit	Does the business have processes and/or procedures for periodic audits of all IP assets and portfolio optimization, portfolio pruning, possible divestitures?
IP policy and education	Does the business have processes and/or procedures for periodic IP rights and IP policy and education trainings for employees?

Source: the authors.

IP strategy checklist

1. **IP awareness and research:**

- understand the basics of IP rights (patents, trademarks, copyrights and trade secrets); and

- research competitors and potential infringements, and ensure mobile app is unique and does not infringe existing IP.

2. **Mobile app documentation**:

- thoroughly document the mobile app's development process, including concept drafts, wireframes and version histories, which will be crucial for potential patent applications and evidence of originality.

3. **Trademark mobile app's name and logo**:

- conduct trademark search to ensure the mobile app's name or logo is not already in use; and
- register the trademark to protect brand identity and avoid potential disputes.

4. **Evaluate patent potential**:

- if your mobile app has a unique functionality or method, consult a patent attorney to explore potential for patenting.

5. **Implement trade secret protocols**:

- for proprietary algorithms or unique processes, establish internal protocols to ensure they remain confidential.

6. **Licensing strategy**:

- decide whether you will license your mobile app or its features to third parties, which can be a revenue stream and also attract potential investors.

7. **Seek nondisclosure agreements (NDAs)**:

- before discussing your app with potential investors, partners or employees, have them sign an NDA to protect your ideas and information.

8. **Develop a business plan highlighting IP**:

- outline how your IP gives you a competitive advantage in the market, which will be crucial for attracting investors.

9. **Regular IP audits and updates**:

- as your mobile app evolves, regularly review IP strategy (update trademarks, consider filing for additional patents, and always keep an eye on the competitive landscape to ensure you remain protected).

Case study: the success of SuperTuxKart in China

Introduction

SuperTuxKart, an imaginary mobile racing game, had successfully garnered a significant number of downloads in Western markets. Seeing the potential in Asia, the app owner sought to enter the Chinese market.

Asia is a vast and diverse continent but one commonality is the rapid adoption of mobile technology. Mobile apps have a vast market, and there is a significant incentive for app owners to fund and monetize their creations. IP can be an asset in this process.

1. Trademark registration

Before entering the Chinese market, the app owner took steps to register their trademarks locally. They knew that China operates on a "first to file" rather than a "first to use" system, meaning whoever files for the trademark first gets the rights, irrespective of who used it first.

2. Licensing deals

With the popularity of their game in other regions, SuperTuxKart's IP became highly valuable. The app owner partnered with local Chinese companies for merchandise. They licensed the IP to create toys, clothing and even snack items, using the game's characters and imagery.

3. In-app purchases and localized content

The owner localized the app's content, providing not just a translation but also culturally relevant characters and tracks. They also created exclusive in-app purchases tied to local events and holidays, further embedding their IP in the culture.

4. Strategic IP collaborations

The app owner collaborated with local brands to introduce crossover events, which increased SuperTuxKart's appeal and provided revenue-sharing opportunities.

5. Enforcement of IP rights

To ensure their IP remained protected, the app owner kept a local legal team on a retainer to monitor and act against any potential infringements, which are relatively common in booming tech spaces.

Takeaways

SuperTuxKart, due to these strategies, became one of the most downloaded games in its category in China. Revenue generated from licensing deals and in-app purchases funded further development and marketing of the app. The protection and strategic use of their IP played a crucial role in securing their brand's position and funding their expansion in the Chinese market.

7.3. IP audit, valuation and market analysis

7.3.1. IP audit

What is an IP audit, and why is it essential? While it may seem like a daunting task, the upside is undeniable, revealing the true value of the app, and often showing it is worth more than initially perceived. And the added bonus? After an initial audit, regular check-ins on the IP become more straightforward, which is empowering in terms of effectively planning and strategizing features and updates. [37]

What: An IP audit is a thorough examination of all the intellectual assets that an app owner possesses, including registered and unregistered rights. Unlike tangible assets, these are outcomes of innovation and creativity, such as business names, trademarks, inventions, product designs, written documents, client lists and trade secrets. The source of these rights might be internal or acquired through contractual agreements with original creators.

Why: Conducting an IP audit offers several benefits:

- recognizes all intangible assets;
- estimates the app owner's overall worth;
- pinpoints business risks;
- facilitates corrective measures and policy development;
- enhances IP asset management and revenue generation;
- supervises adherence to contractual commitments; and
- ensures protection and enforcement of IP rights.

When: Ideally, app owners should undertake an IP audit annually, aligning it with their financial year-end or start. However, special occasions such as business mergers, expansions or seeking a loan might necessitate additional audits or updates.

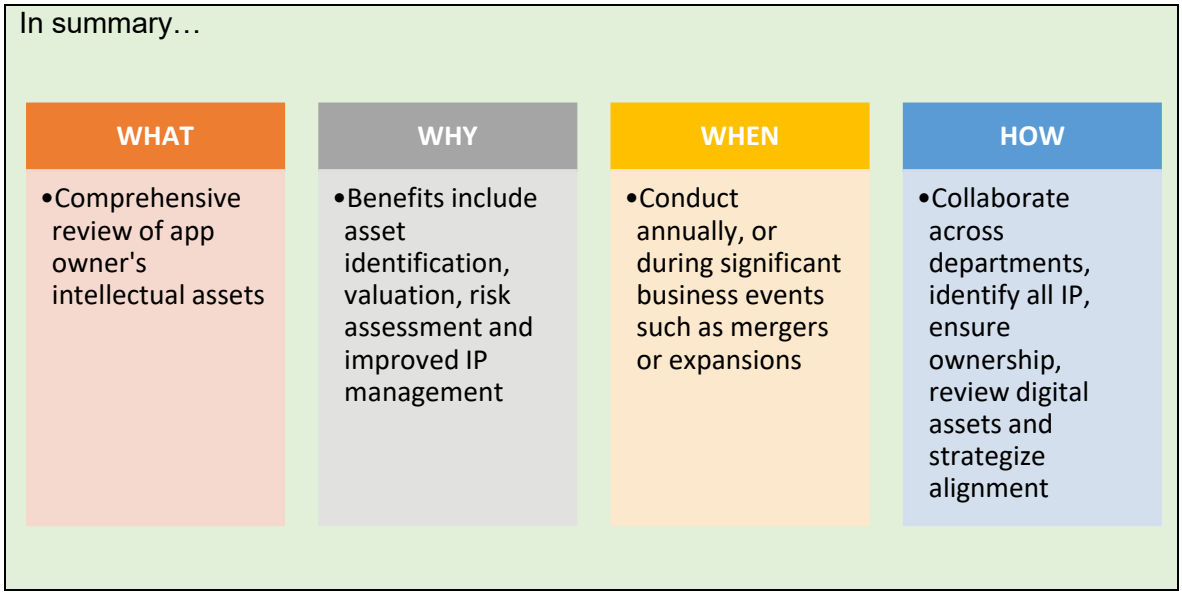
---

[37] More information on IP audits is available on the WIPO website, www.wipo.int/sme/en/ip-audit.html.

How: The process involves collaboration, often requiring insight from multiple departments and possibly external legal or technical experts. Steps include:

1. assessing all business dimensions for IP relevance;
2. identifying, verifying and documenting all IP rights;
3. ensuring rightful ownership and usage permissions;
4. evaluating potential IP rights violations;
5. reviewing digital assets such as websites;
6. Strategically aligning IP rights with business objectives and
7. preparing for future technologies such as blockchain for more straightforward audits.

Figure 7.2 Steps for an IP audit



Source: the authors.

How to identify IP in my mobile app?

The following IP identification checklist will serve as a guide to analyzing the essential aspects that will enable you to identify your mobile app's IP, and determine whether it is properly protected.

Checklist: IP identification
1. App general information

1.1 App name:

1.2 Version:

1.3 Release date:

1.4 Developer/team name:

2. App design

2.1 Have you used any proprietary designs or graphics within the mobile app?

☐ Yes

☐ No

2.2 If yes, please specify or provide samples.

2.3 Are there any unique user interface (UI) elements or user experience (UX) flows that have been specially designed for this mobile app?

3. App code

3.1 Is the codebase developed entirely in-house, or are there any third-party integrations?

☐ Entirely in-house

☐ Third-party integrations

3.2 If third-party integrations are used, please list them and specify if they are open source or licensed.

3.3 Are there any unique algorithms or proprietary code sequences developed specifically for the mobile app?

4. App content

4.1 Does your mobile app include copyrighted content (for example, music, videos, text)?

☐ Yes

☐ No

4.2 If yes, please specify the type of content and its source.

4.3 Are there any patents associated with the mobile app or its functions?

5. Trademarks

5.1 Is the mobile app name or logo trademarked?

☐ Yes

☐ No

5.2 If yes, please provide the trademark registration details.

6. Licensing

6.1 Does the mobile app use any software or content under specific licenses?

☐ Yes

☐ No

6.2 If yes, please provide details of the licenses, including any obligations or limitations they impose.

7. Data and user information:

7.1 Does the mobile app collect user data?

☐ Yes

☐ No

7.2 If yes, is any of the data proprietary or used in a unique manner that could be considered IP?

8. Collaborations and partnerships

8.1 Were there any collaborations or partnerships involved in the development or distribution of the mobile app?

☐ Yes

☐ No

8.2 If yes, please list the entities and describe the nature of the collaboration.

9. External contributors

9.1 Were there any external contributors (freelancers, contractors) involved in the mobile app development?

☐ Yes

☐ No

9.2 If yes, do you have agreements in place regarding IP ownership and rights? Please elaborate.

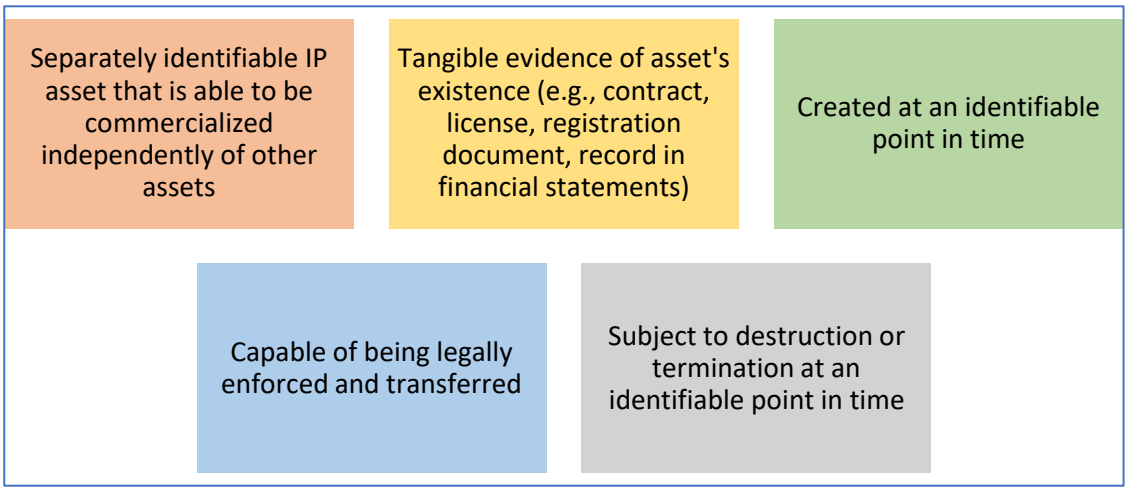
7.3.2. IP valuation

Companies in the mobile app industry base their operations on intangible assets and innovation, and may be more likely to thrive if the IP is correctly identified and valued. IP valuation can help determine the true value of a business (and app owner as a whole) and leverage assets that may be unaccounted for or underutilized to maximize their profitability.

Therefore, for app owners, evaluating the worth of the intellectual assets is crucial in various scenarios. Determining the value of patents, trademarks, copyright and trade secrets simplifies the process of licensing or transferring those assets, enabling suitable usage fees to be set when others wish to utilize them. Moreover, an IP valuation can enhance the app owner's financial standing, paving the way for better funding opportunities. For emerging mobile app companies, having or pursuing formal intellectual rights is often linked with increased external funding. A knowledgeable IP valuation of these assets can effectively convey their worth to potential investors.

WIPO's Valuing Intellectual Property Assets sets out several prerequisites for an IP valuation (also see figure 7.4).

Figure 7.3 Prerequisites for valuing an IP asset



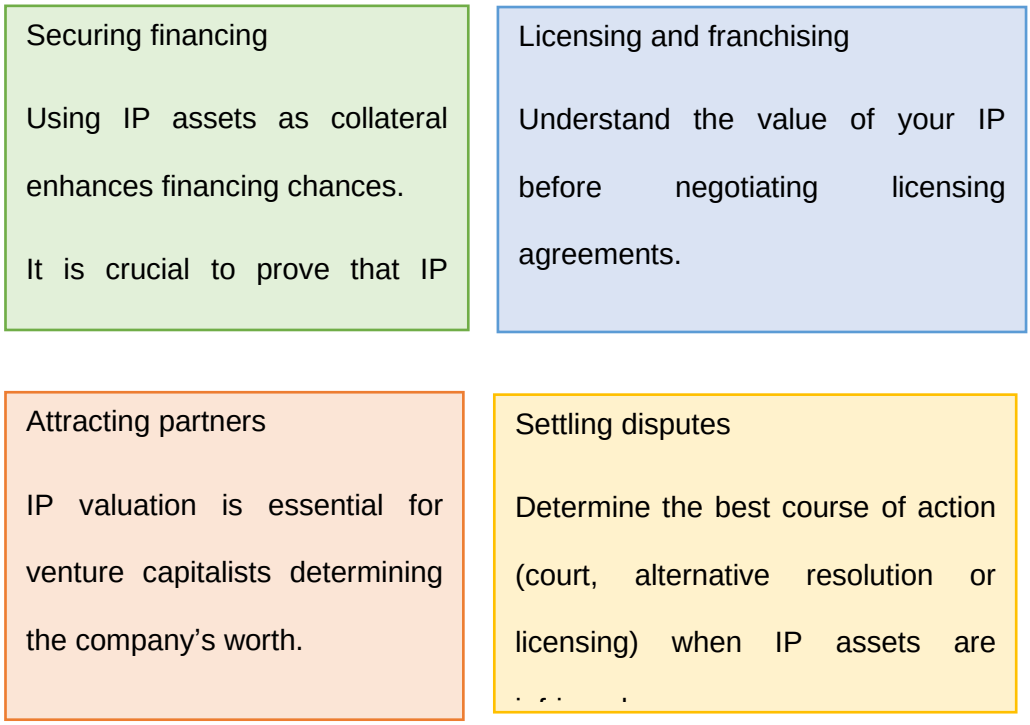
Source: the authors.

The general principle governing the valuation of IP is the degree of competitive advantage that the app owner's IP provides relative to other companies in the industry – in this case, the IP relating to the mobile app. Although this question can be approached from many perspectives, valuation methods are generally divided into two broad categories: qualitative valuation or quantitative valuation.

IP valuation in practice

To learn more about IP valuation, we recommend reading WIPO's module 11 on IP valuation. In practice, IP valuation can be grouped into broad categories (see figure 7.5).

Figure 7.4. IP valuation in practice



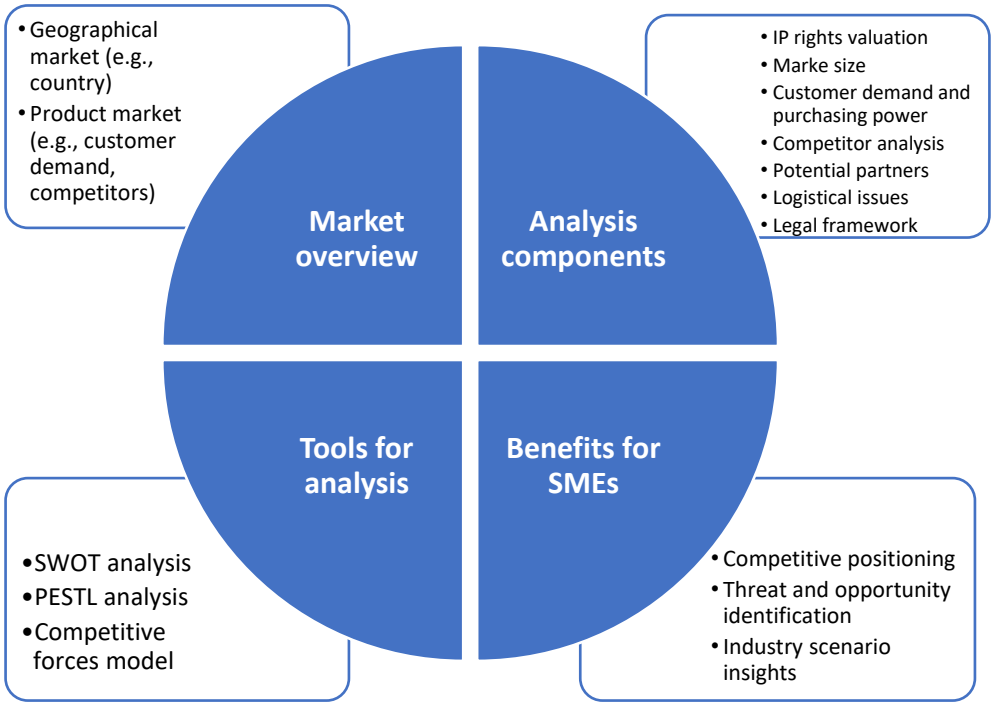
Source: the authors.

a) Market analysis

For the effective valuation and commercialization of IP, it is essential to undertake a comprehensive market analysis. This includes understanding both the geographical region and the specific product market. Important elements of this analysis include IP rights valuation, market size, customer demand, purchasing power, competitor presence and capacity, potential business partners, logistical considerations and the relevant legal framework. SMEs benefit from such an analysis as it provides clarity on their competitive position, potential threats and opportunities, as well as insights into industry scenarios.

Three tools for effective market analysis are SWOT, PESTLE and the competitive forces model. Each provides unique insights into an app owner's standing, external factors influencing their business and the competitive landscape.

Figure 7.5 Key factors when performing market analysis



Source: the authors.

b) Comparing SWOT and PESTLE analyses

SWOT examines specific strengths, weaknesses, opportunities and threats, while PESTLE identifies the broader external environment, including political, economic, social, technological, legal and environmental factors (see table 7.7).

Table 7.2 Comparing SWOT and PESTLE

SWOT analysis	**PESTLE analysis**
SWOT analysis is a strategic planning tool that helps a company or individuals evaluate internal strengths, weaknesses, opportunities and threats. - **Strengths**: internal factors that give an advantage over competitors	PESTLE analysis is a strategic planning tool that helps a company or individuals understand the external macroenvironmental factors that might affect their work or decisions.

- includes skilled development team, proprietary technology or algorithms, positive user reviews and ratings, and strong brand identity in the app market.
- **Weakness**: internal factors that could place the company at a disadvantage compared with competitors
  - includes limited funding for development, slower update cycles compared with competitors, lack of integration with popular third-party services, and inexperience in a particular mobile app category.
- **Opportunities**: external factors the company can exploit to its advantage
  - includes emerging markets or user bases, integration with new tech (e.g., AR/VR), wearables, partnerships with other tech companies/platforms, trends in user needs and behaviors (e.g., health and fitness, remote work).
- **Threats**: external factors that could cause trouble for the business
  - includes increased competition in the app store, changes in app store policies or revenue splits, technological advancements that render the app obsolete, negative publicity or security breaches.

Once these four elements have been identified, the next step is to devise strategies that leverage strengths and opportunities while addressing weaknesses and mitigating threats.

It is good practice for app owners to periodically revisit their SWOT analysis, especially when entering new markets, launching new products or facing significant industry changes.

- **Political**: refers to the impact of government policies, regulations and political stability
  - includes data privacy laws (e.g., GDPR, CCPA), censorship and content restrictions, import/export regulations and IP rights.
- **Economic**: involves economic growth, inflation rates, exchange rates and overall economic health
  - includes purchasing power of target users, economic stability affecting user spending, potential for in-app purchases/premium versions, and exchange rates for global apps
- **Social**: refers to the demographic, cultural and societal norms and changes
  - Includes cultural preferences and sensitivities, population demographics and tech literacy, trends in social media and communication and shifts in user behaviour and needs.
- **Technological**: involves technological advancements and innovations
  - includes emerging tech trends (e.g., AR/VR), device compatibility and OS updates, cybersecurity threats and measures, cloud technologies and server capacities.
- **Legal**: refers to the laws and regulations that businesses must comply with
  - includes mobile app content regulations, copyright and

	trademark concerns, contractual obligations with partners/providers and employment laws for developer teams. - **Environmental**: pertains to ecological and environmental concerns - includes energy consumption of apps, electronic waste and device recycling, impact of server farms on environment and corporate social responsibility initiatives. App owners, especially those in the educational sector, can utilize this tool to identify external factors that might influence the app's success. By integrating PESTLE analysis into their planning and development process, owners can make informed decisions that ensure their apps are technologically sound and also socially, legally and environmentally attuned.

Source: the authors.

7.4. IP commercialization

Acknowledging IP as a key part of the mobile app, and creating a protection and exploitation strategy, is crucial to attract investors and secure funding. However, it is not the only way IP can be monetized. Most often, commercialization of the mobile app itself (under different sales models) is the primary objective for generating revenue.

In the IP context, commercialization implies bringing IP to the market to generate a profit.

In this section (complementing chapter 3, Income streams in the app industry), the main IP commercialization models will be presented.[38]

Which commercialization model is appropriate?

It is important to take a moment and ask a few questions to determine the model that is most suitable.

Doing it by yourself? The direct licensing model

In this case, the IP remains yours and you can make sales directly or through a distributor.

- Licensing the mobile app or selling the mobile app services directly to consumers.
- Selling through a distributor.

Letting third parties use your IP? The indirect licensing model

- If you authorize another person or company to use your IP rights through licensing agreements, in exchange for a fee.
- In this case, you must enter into a license agreement and allow the licensee to do the work (distribute and promote your app through marketing) instead of you.

Selling the IP? The assignment model

- You can sell your mobile app.
- Transfer the IP in exchange of a lump-sum fee.

Sharing activities with someone? The partnership model

- You will need to identify where it is beneficial for you to leverage the capabilities of another company to support your business objectives.
- Ensure that you enter into agreements to determine how current and new IP will be managed with a strategic partner.

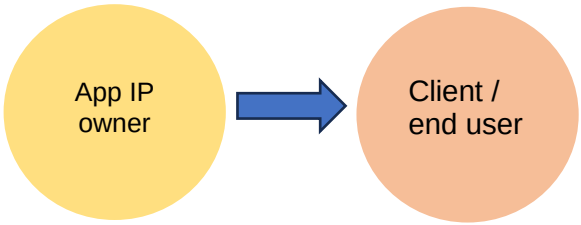
7.4.1. Commercialization by the IP owner

[38] More information is available in WIPO, WIPO Tool on the Financing of Intellectual Property-based Mobile Apps, 2021 <www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo-tool-financing-mobile-apps.pdf>.

When app owners decide to commercialize their mobile apps independently, they take charge of the entire process – from ideation and development, to marketing and distribution. There are several reasons why an owner might opt for this solo route, including:

- possess existing robust marketing strategy and capability;
- lack the bandwidth to form or nurture partnerships;
- reluctant to share proprietary mobile app information with external parties; and
- desire to avoid potential competition or the time and investment required to establish partnerships.

Figure 7.6 Commercialization by IP owner



Source: the authors.

Choosing this path allows app owners to retain total control over their mobile apps (and corresponding IP). This means they not only have the power to make all decisions but also stand to reap all the profits. While this sounds enticing, it is essential to recognize that going solo might not always result in a competitive edge. Collaborative efforts can bring diverse skills and perspectives, potentially enhancing the mobile app's appeal and functionality. Those who can manage the journey alone, however, get to keep all the rewards.

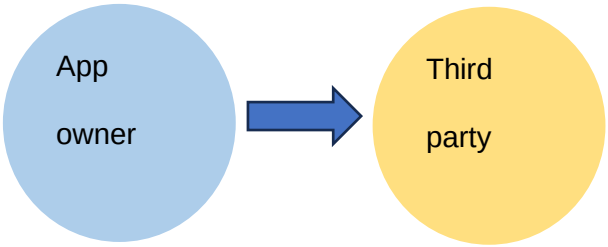
7.4.2. Licensing

One of the most effective ways to extract value from IP assets such as patents, trademarks, or datasets is through an outbound licensing model. This involves granting

permission to third-party entities to utilize one's IP in exchange for compensation, typically in the form of licensing fees or royalties.

Outbound licensing is essentially the act of allowing another party to leverage your IP for their endeavors. Rather than internally commercializing an IP, rights holders can license it out, potentially generating continuous streams of revenue. This is especially prevalent in the mobile app sector, where technologies, brand names and datasets can be licensed to other pp owners seeking to build on existing innovations.

Figure 7.7 Licensing model



Source: the authors.

For mobile app owners, the outbound licensing model offers a multifaceted approach to leveraging their IP. First, it presents an avenue for (often recurring) monetization. Developers can seamlessly earn royalties from their IP, eliminating the need to divert additional resources for product or service deployment. This offers a financial advantage and also ensures continued innovation without capital constraints.

Second, this model aids risk reduction. Licensing out IP means that the complexities and challenges of commercialization are borne by the licensee. This is especially beneficial for app owners who may not possess the requisite infrastructure or resources to roll out the IP on a grand scale.

Finally, and perhaps most significantly, it fosters collaboration. Licensing can act as a bridge, connecting two entities with shared or complementary visions. This often culminates in synergetic partnerships where the combined skills and assets of both

parties lead to the creation of a product or solution that is far more competitive and groundbreaking than if developed in isolation.

More information on license agreements and their key terms is available in chapter 5, IP contracts in mobile apps, and the *WIPO Tool on the Financing of Intellectual Property-based Mobile Apps*.

Case study: Outbound licensing in mobile app development – The success of AppTech Innovations

Background

AppTech Innovations, a small start-up founded by a group of mobile app owners in the Philippines, created a groundbreaking algorithm to enhance real-time AR interactions within apps. At the time, the algorithm's capability to seamlessly integrate the physical and digital worlds in real-time was unparalleled. But AppTech faced challenges. It possessed a revolutionary technology but lacked the financial muscle and market reach to fully commercialize the innovation on a global scale.

Objective

To maximize the value and reach of their AR algorithm without incurring the heavy costs and risks associated with large-scale commercialization.

Solution

AppTech decided to adopt an outbound licensing model for their proprietary AR algorithm, which included the following steps:

1. Monetization: recognizing the potential value of their innovation, AppTech entered into licensing agreements with multiple established AR game developers, allowing them to integrate the algorithm into their games. This resulted in a steady stream of royalty income for AppTech, ensuring financial sustainability.
2. Risk reduction: the decision to license the technology meant AppTech was not directly responsible for the mass-market deployment and commercial risks associated with the algorithm's broader integration. The game developers, as licensees, took on the burden of integrating the algorithm into their games, managing user feedback and ensuring market success.

3. Collaboration: one licensing agreement evolved into a strategic partnership with GamerWorld Inc., a giant in the industry, and together, they codeveloped a game that became a massive hit globally. AppTech's algorithm combined with GamerWorld's expertise in design and market reach proved a winning formula.

Outcome

AppTech's decision to utilize the outbound licensing model proved a masterstroke. Within two years:

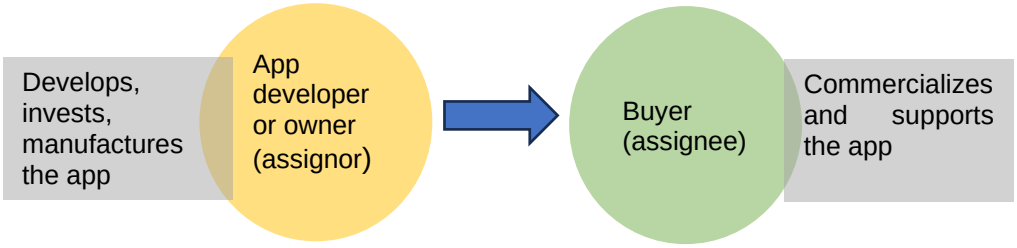
- The AR algorithm was integrated into five top-selling AR games worldwide.
- Royalty revenues exceeded initial projections by 150 per cent, allowing AppTech to reinvest in R&D and come up with more innovations.
- The strategic collaboration with GamerWorld resulted in the codevelopment of the game RealmFusion, which secured the top spot in global AR game charts for six consecutive months.

AppTech showcased the potential of the outbound licensing model in mobile app development. By licensing their groundbreaking algorithm, they not only ensured a lucrative revenue stream but also positioned themselves as innovators in the competitive AR market, while also minimizing risk and fostering industry collaborations.

7.4.3. Assignment

IP assignment is one of the commercialization models in the mobile app sector where an app developer, or owner or company, transfers all rights, titles and interest in their app to another party, typically a company or investor. This is comparable to selling the blueprints of a product, ensuring the recipient has full ownership and control over the app's future direction, monetization strategies, and any derivative works.

Figure 7.8 Assignment model



Source: the authors.

There are numerous positives to this model: app owners can get immediate financial returns, mitigate future liabilities related to the app and avoid the complexities of long-term mobile app management or marketing. Additionally, for owners lacking the resources or know-how to bring a mobile app to its full market potential, IP assignment can present a favorable way to ensure their creation reaches a broad audience. But the model is not without its drawbacks. Apart from the difficulty of performing the IP valuation process, owners relinquish all future profit potential and lose any say in the app's future development, and, if the app becomes wildly successful, may feel they sold their rights too cheaply.

It is essential that app owners weigh these pros and cons carefully, possibly with legal consultation, before choosing to assign the IP rights.

Assignment Tip

It is important to have the assignment details in writing and to ensure the records of the corresponding IP offices are up to date at the moment of transferring the IP to the other party. Consider the following:

- What is the purpose of the assignment?
- What are the IP assets that will be involved in the sale?
- Who will own any new IP that may be created?
- Is each party the rightful owner of the IP and/or does each party hold the necessary rights to the IP of third parties?
- Has an IP valuation been performed on the IP to be transferred?

7.4.4. Partnerships or joint ventures

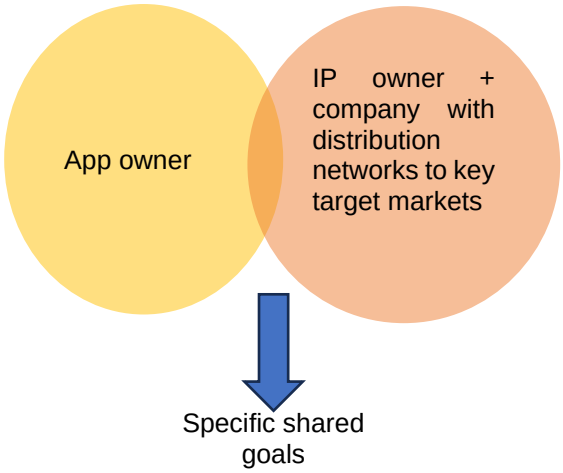
A partnership or joint venture serves as a leading commercialization model for mobile app owners seeking to combine resources, expertise and market reach.

Given that the other models discussed may be too large for a small company (which may be at an incipient stage), this partnership or joint venture model involves joining forces to promote a common project. Two or more entities collaborate to design, develop and monetize a mobile app.

The primary advantage of such an approach lies in the pooling of resources – financial, technical and operational – thereby reducing individual risk and leveraging collective strengths. Further, it provides a shared platform for diverse expertise, potentially leading to innovation and enhanced mobile app functionality. This model also ensures broader market access when partners have varying user bases or regional influences.

On the downside, partnerships require comprehensive coordination and clear communication to avoid misunderstandings. The division of profits might be a point of contention, and the pace of decision-making can be slower due to the need for consensus. Additionally, IP rights and operational roles need to be clearly delineated to prevent future disputes.

Figure 7.9 Partnership or joint venture model



Source: the authors.

In conclusion, while partnerships and joint ventures in the mobile app sector offer combined strength and shared risk, they require clear agreement and understanding among all parties.

In this model, critical information of great strategic value is disclosed, and it is advisable to sign an NDA and perform due diligence, where certain common questions should be asked of the potential partner.

The differences between a partnership and a joint venture are explained in detail in table 7.3.

Table 7.3 Partnership or joint venture

	Partnership	**Joint venture**
Definition	An association of two or more parties to run a business together with shared profits and losses.	A business arrangement in which two or more parties collaborate for a particular project or a set period.
IP ownership	Usually jointly owned by partners unless otherwise specified.	Typically created for the specific joint venture project and can be jointly owned or retained by individual parties based on the agreement.
IP management	Managed collectively unless a different structure is set in the partnership agreement.	Managed as per the terms of the joint venture agreement. Can be centralized or distributed.
Flexibility	Tends to have broader scope, encompassing various business activities.	More focused, typically centred on a single project or goal.
Profit and loss sharing	Shared among partners as per the agreed ratio.	Shared as per the terms of the joint venture, which might differ from traditional partnerships.
Duration	Often undefined. Can continue as long as partners agree.	Typically for a defined period or until a particular project is completed.
Risk and liability	Partners usually have joint liability.	Defined by the joint venture agreement. Can be joint or several depending on the terms.

Source: the authors.

There are other ways to obtain revenue – selling mobile app licenses, for instance. For a complete picture of the different revenue sources in the mobile app industry, see chapter 3, Income streams in the app industry.

Case study: joint venture for mobile game commercialization

Scenario

The game developer TechTonic has designed a groundbreaking game but lacks the resources to distribute and market it at scale. PlayMob, a large mobile game publisher, has extensive reach and expertise in game marketing and distribution.

Actors

- TechTonic (app owner).
- PlayMob (app publisher).

Steps

1. Discovery and negotiation: TechTonic approaches PlayMob with its unique game IP. Both parties discuss potential collaboration and revenue share.
2. Partnership formation: TechTonic and PlayMob formalize a joint venture, outlining terms of IP usage, commercialization strategy and profit distribution.
3. Integration and distribution: TechTonic shares game files and assets. PlayMob integrates the game into its distribution network, handling marketing and in-app transaction mechanisms.
4. Performance monitoring: PlayMob provides TechTonic with analytics, feedback and revenue reports. The parties collaborate to refine the game based on user feedback.
5. Revenue distribution: profits from game sales and in-app purchases are split as agreed (for example, 60/40).
6. Review and renewal: on reaching the three-year mark, the parties review performance. If both are satisfied, the partnership can be renewed or renegotiated.
7. Optional exit: if revenue targets are not met by year two, either party has the option to terminate the partnership.

8. Takeaway: by combining TechTonic's innovative IP with PlayMob's extensive distribution network, the game achieves larger market reach, and greater recognition and potential profitability for both parties.

7.5. Conclusions

In the rapidly evolving mobile app industry, the value of an app goes beyond just its code and design. The IP encapsulated within an app holds tremendous potential for financing, monetization and strategic leverage. For app developers and owners, recognizing and maximizing this potential is not just a luxury but a necessity.

To benefit from IP, the following steps are imperative to maximize the IP portfolio relating to the mobile app:

- **IP audit**: the start and foundation of this journey is the IP audit. With a systematic identification of every intellectual asset, it provides a clear view of what sets the mobile app apart, ensuring it is protected and highlighted to stakeholders.
- **IP valuation**: beyond identification, understanding the financial worth of these intangibles ensures app developers and owners are well prepared and confident in negotiations, ensuring they secure the funding their innovation merits.
- **Market analysis**: equipped with knowledge about the mobile app's IP, positioning it correctly in the vast mobile app ecosystem is crucial. A robust market analysis highlights trends and competitors, and also pinpoints where the app's unique IP provides a competitive advantage.

Further, IP commercialization provides strategic avenues for monetization:

- Direct or indirect licensing, perhaps the most flexible, ensures a continuous revenue stream, allowing for expansive reach while retaining ownership.
- Assignment offers a direct route for capital influx through the sale or transfer of IP rights.

- Partnership or joint venture lays a path for synergistic growth, leveraging combined strengths and IP assets.

The journey of a mobile app, from conception to commercialization, is filled with challenges. However, with tools like IP audit, IP valuation and market analysis, app owners are equipped to adeptly navigate this journey. They can not only protect their invaluable intangible assets but also carve out strategic partnerships, joint ventures and licensing models to ensure the mobile app's longevity and profitability.

In essence, leveraging IP is not just about protection, it is about recognizing and capitalizing on the true worth of a mobile app. For app owners willing to delve deep into the world of IP, the rewards, financial and strategic, can be transformative.

Key takeaways

- Elaborate an IP strategy, allowing the app owner to know their IP assets and adequately protect and make the most of their commercialization.
- Ensure IP audits are performed on regularly over time.
- Perform IP valuation and market analysis when a new IP asset is identified.
- Analyze the most convenient commercialization model considering the current needs of the business.

7.6. Useful links and resources

WIPO: The IP toolbox for mobile App Owners: 2021 <https://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo_ip_toolbox_mobile_apps.pdf>

WIPO, *The Role of Intellectual Property Rights in the Development and Commercialization of Mobile Applications*. 2021. https://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo_iprs_mobile_apps.pdf

WIPO, *Protecting Your Mobile App: Intellectual Property Solutions. 2021 https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1071.pdf*

WIPO, *WIPO Handbook on Key Contracts for Mobile Applications: A Developer's Perspective*. 2021 https://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo_handbook_key_contracts_mobile_apps.pdf

WIPO, *Uncovering IP Risks and Potential: IP Audit*. Visited March 2024 http://www.wipo.int/sme/en/ip-audit.html

WIPO, *Valuing IP assets*. Visited March 2024 https://www.wipo.int/sme/en/ip-valuation.html

WIPO, *IP Financing: The Ten Commandments*. Visited March 2024. <http://www.wipo.int/wipo_magazine/en/2008/05/article_0002.html>

WIPO, *Securing financing with IP assets*. Visited March 2024 https://www.wipo.int/sme/en/securing-financing.html

Chapter 8. Protection of personal data in mobile apps

8.1. Introduction

This chapter outlines the main aspects that must be understood and applied in the life cycle of a mobile app in order to comply with privacy regulations, and how to correctly apply the privacy by design (PbD) principle while implementing the appropriate security measures.

The number of parties and personal dataflows that may take place during that app life cycle, particularly when apps are made available to end users, and the multiple legal regimes where the app may be managed or provided, makes for a complex scenario. In addition, while the European Union's GDPR remains leader of the field, more countries are adopting privacy legislation due to the increasing amount of data processed and level of sensitivity. Further, the rise of technologies such as machine learning and AI have introduced new processing that may put the rights of users ('data subjects' in European privacy language) at risk if appropriate safeguards are not adopted.

The exponential growth of the mobile app market and the consequent processing of personal data has increased the likelihood of unauthorized exposure of personal data, or processing done in an opaque, illegitimate manner without respect for the rights of users. Hence, concerns have become a reality, and governments around the world –led by the European Union and countries such as Canada and Japan – have adopted regulations to ensure processing carried out through mobile apps respects fundamental privacy principles.

It is essential to raise awareness among key parties, particularly app owners, of the crucial role played by data protection rights and obligations, to understand which aspects must be considered and guaranteed, from the conception of the app idea to its deployment on the end user's mobile device.

A high-level overview of the flows of personal data that usually occur in the life cycle of an app will be provided. The roles played by key parties in terms of data protection in

this cycle will be presented, highlighting their respective obligations and responsibilities and providing recommendations these parties must consider in order to be diligent in processing personal data and to comply with regulations. Further, from a practical perspective, we will identify some of the main risks, as well as the legal instruments and recommendations to mitigate them, that may arise in terms of data protection.

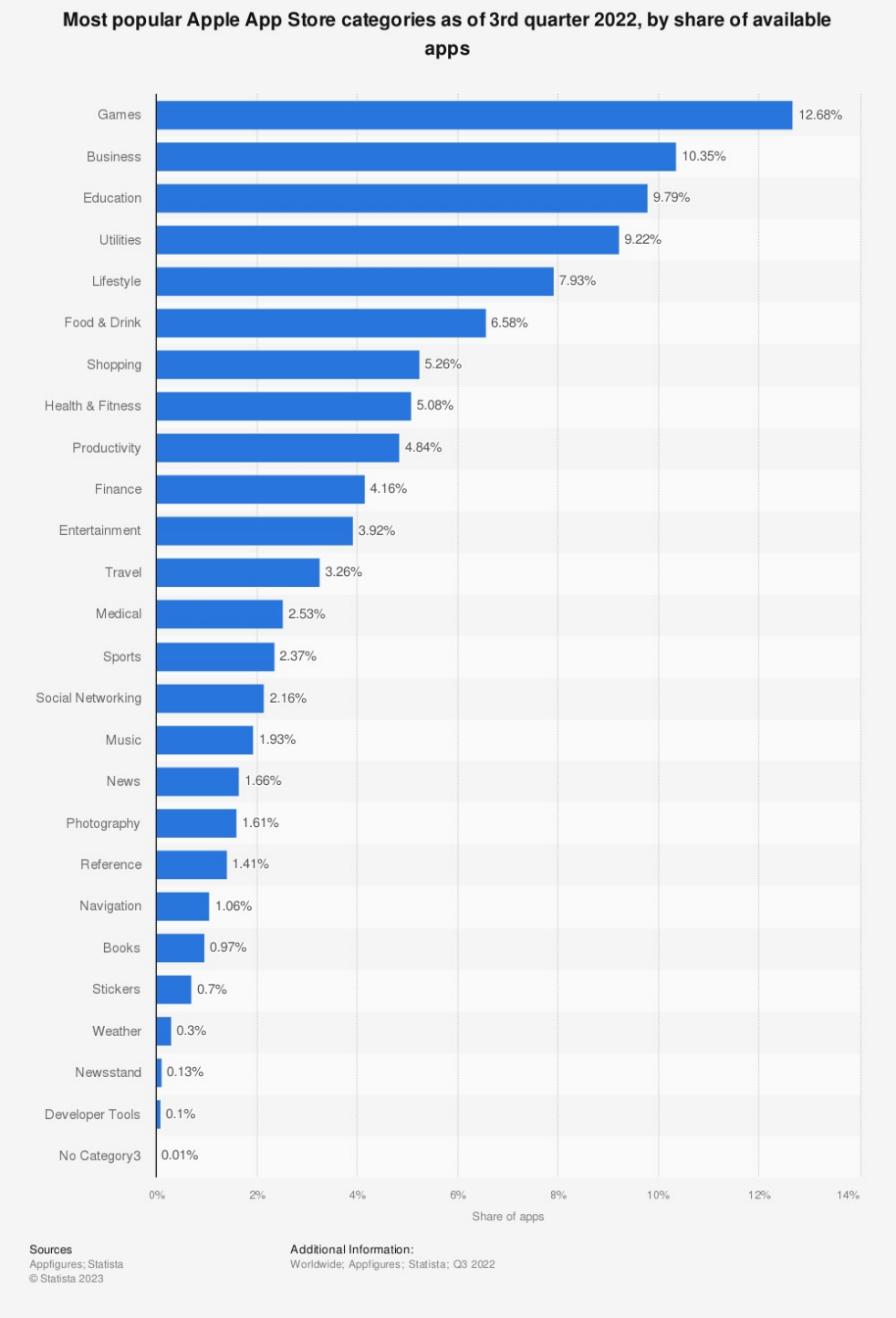
Finally, this chapter presents the principles of privacy by design and privacy by default, and their critical role in mobile app development. These principles emphasize that privacy should not be an afterthought in the development process but a guiding design factor, integrated from the conception phase. The chapter looks at how app owners and/or developers or agencies (if applicable) can design mobile apps with a privacy-centric mindset, from planning to the development, testing and deployment phases.

More detailed information is available on the WIPO website, www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo-guide-data-protection-mobile-apps.pdf.

8.2. Context and legal framework

In chapter 1, we discussed the astronomical rise in the number of mobile apps being used worldwide, such that they have become an integral part of our daily lives. The apps most downloaded by end users are entertainment and social networks, where data obtained are not a priori sensitive (such as health data or criminal records), although the vast quantity of data processing makes privacy a key aspect. Practices with an important impact on privacy for end users have been detected, such as the massive quantity of data processing, transfer of complex data with third parties and international cross-border transfers.

Figure 8.1 Most popular app store categories, June 2021



Source: Statista. “Most popular Apple App Store categories as of 3rd quarter 2022, by share of available apps.” *statista.com.* Dec. 8, 2023. <www.statista.com/statistics/270291/popular-categories-in-the-app-store/>.

In addition, health and lifestyle, and finance apps are increasingly integrated into our lives to perform any procedure, and if app owners do not satisfy privacy and security requirements, they exponentially increase the likelihood of breaching personal data

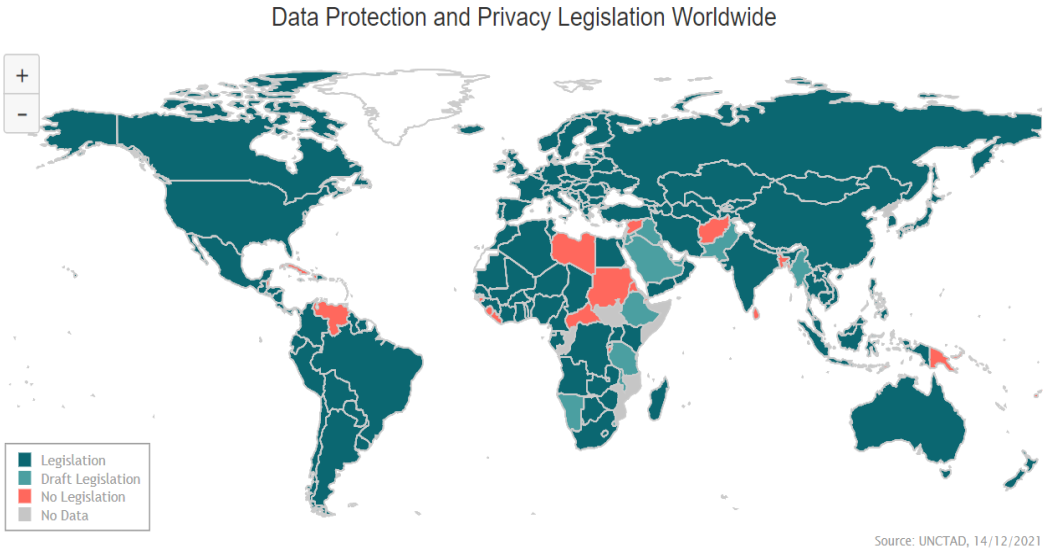
protection regulations and end-user rights. During the first quarter of 2023, it was estimated that, worldwide, more than six million data records were exposed through data breaches. Since the first quarter of 2020, the highest number of exposed data records was detected in the fourth quarter of 2020, with nearly 125 million datasets.

As mobile data consumption continues to experience exponential growth, concerns over data processing have come to the attention of users and data protection authorities around the world, with many expressing their intention to redouble privacy enforcement efforts. Mobile apps are undeniably and increasingly becoming the main gateway to online services, and governments acknowledge the need to ensure compliance with data protection rules.

According to the United Nations Conference on Trade and Development (UNCTAD), "*137 out of 194 countries have legislation to safeguard individual data and privacy. Africa and Asia show a different level, with 61 per cent and 57 per cent of countries, respectively, having adopted such legislations. In the least developed countries, the share is 48 per cent"*.[39]

[39] United Nations Conference on Trade and Development. "Data protection and privacy legislation worldwide." *Source: unctad.org.* 2021. Data protection and privacy legislation worldwide <www.unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

Figure 8.2 Data protection and Privacy legislation worldwide



Source: UNCTAD, Data protection and privacy legislation worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

The GDPR is arguably the most implemented and influential personal data protection regulation in the world. Its global impact arises from its extraterritorial scope, meaning that even companies outside the European Union must adhere to its regulations when dealing with EU citizen data. Following the introduction of the GDPR, several countries and regions have introduced or revised their own data protection laws.

In contrast to this harmonized regulation, in the United States of America there are specific state laws, including, for example, the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (CDPA), that have introduced strict requirements for companies operating in those states, which may affect app owners providing services to state residents. It should also be noted that app owners may also be subject to industry-specific federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA) for health-related information, or the Children's Online Privacy Protection Act (COPPA) for apps targeting children under the age of 13. To avoid penalties and maintain end-user trust, app owners must be mindful of this fragmented

regulatory environment, and vigilant in understanding and complying with the patchwork of state and federal requirements.

Asian countries have significantly advanced in terms of privacy regulation. Countries such as Thailand (Personal Data Protection Act, B.E. 2562 of 2019),

Viet Nam (Decree No. 13/2023/ND-CP), Indonesia, Japan (Act on Protection of Personal Information.,2020) and China (Personal Information Protection Law, 2021) have introduced regulations governing the processing of personal data or have updated existing ones.

In general, these regulations have incorporated concepts from the GDPR, including:

- China has integrated the principles on which the GDPR is based (lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitations; integrity and confidentiality; and accountability), the rights of data subjects, and the concept of data controller and data processor, including the need to appoint a data protection officer and local representative in certain scenarios. There are differences; for example, with international transfers and privacy notices, the regulations have gone beyond the GDPR.
- Viet Nam’s data protection law has incorporated the GDPR’s concepts of controller and processor but introduces a new concept of controller and processor, a figure that decides the purposes and the means, as well as directly processing personal data.
- In Indonesia, the passage of the law has included restrictions on cross-border transfers and obliges organizations to ensure that the country to which personal data is exported has a level of data protection equal to or higher than the new Indonesian law.

Likewise, in Latin America, countries have also recently made legislative developments in data protection, such as:

- In Argentina, following a public consultation process, the aim is to update the current law (Law No. 25.326) to harmonize regulations with technological advances and global trends. The amendment takes as its main references the GDPR, Convention 108 of the Council of Europe, and United Nations Educational, Scientific and Cultural Organization (UNESCO) recommendations on the ethics of AI, among others. It addresses the principles of lawfulness, fairness, transparency, purpose, data minimization, accuracy, proactive responsibility and security, and establishes mechanisms for the processing of sensitive data, consent, international transfers, rights of data subjects, responsibilities of actors involved in data processing and penalties for noncompliance.
- In Peru, in August 2023, the Ministry of Justice and Human Rights announced the publication for public consultation of Regulation of Law No.29733 on personal data protection. The proposed law integrates concepts from the GDPR, such as the notification of security breaches, obligation to perform data protection impact assessment and right to data portability.
- Also in August 2023, Colombia's Chamber of Representatives introduced Bill 156/2023C on the General Regime for the Protection of Personal Data, which aims to establish new rules on the protection and processing of personal data. It presents the same principles as the GDPR, including the extraterritorial component, and establishes provisions relating to video surveillance, publicity and ethical guidelines, as well as the integration of rights derived from the use of new technologies such as AI.

Not all laws relating to privacy are general privacy laws but may target specific sectors such as health, biometrics, criminal activities (for example, identity theft) or students. In addition, as mentioned, some laws are extraterritorial to the extent that they apply to mobile apps developed and operated from third countries, targeting the citizens of that

country with privacy laws. This means app owners, particularly those processing large amounts of data or sensitive data, will need to consult a privacy professional to ensure compliance with local and third-country laws.

8.3. Scope, main roles and obligations

Mobile apps are designed to satisfy a variety of needs. To do so they need to access, process and transmit large amounts of personal data, from the seemingly innocuous, including IP address or location data, to the deeply personal, such as medical or financial details. Generally, what counts as personal information is broad, being data relating to identified or identifiable persons.

Examples: personal data

With mobile apps, there is information that falls within the definition of personal data according to existing international regulations,[a] including:

- data collected directly from a user via the mobile app's user interface (name, address, date of birth);
- data gathered indirectly such as mobile phone number, International Mobile Equipment Identity (IMEI) or universal unique identifier (UDID);
- data gathered about a user's behaviour such as location, web-browsing or the mobile apps used that are linked to a unique profile; and
- user-generated data such as contact lists, videos, photos, messages, emails, notes and call logs.

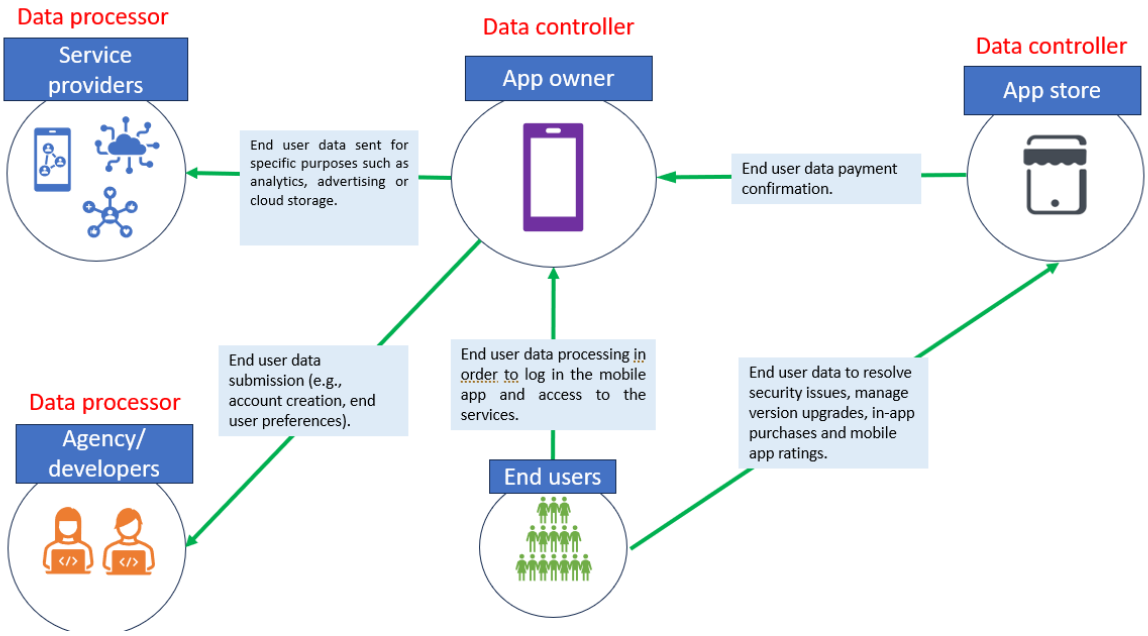
A user does not need to be known by name to be identified. They can be identifiable even if their information is associated only with a unique identifier, such as a UDI.

[a] Convention 108 of the Council of Europe, signed in 1981, regulated for the first time in Europe the concept of personal data. This was developed with the Data Protection Directive – officially Directive 95/46/EC – of 1995, which regulated the processing of personal data and the free movement of such data. The directive defined personal data as any information relating to an identified or identifiable natural person.

Behind many user-friendly mobile app interfaces lies a web of dataflows between the different parties in the app technology platform(s). Such flows encompass the app's

interaction with third-party integrations, service providers (cloud storage, ad networks, analytics providers, among others) and app stores.

Figure 8.3 Personal dataflows when an end user runs a mobile app



Note: GDPR terminology of controller and processor

Source: the authors.

First, we must understand the main data protection roles that determine the obligations of the key parties acting under those roles.

What are the main roles in terms of data protection?

Many legislations have adopted the European Union's GDPR terminology (or similar) and framework for describing the roles of persons and entities in data protection and their rights and obligations. This is not universal, however, and local advice should be sought.

Data controller (or personal information controller)

The data controller is the individual, company or other body who determines the purposes and means of processing personal data. They decide why the data is being processed and how it will be done**.**

So, if you are creating an app (as an app owner or an app publisher) and you are deciding what data to collect from users and how to use it, you are acting as a data

controller. This entails specific responsibilities, such as ensuring the data is processed lawfully, transparently and for a specific purpose. You are also responsible for protecting the rights of the data subjects.

Data processor (or service provider)

A data processor is an individual, company or other body who processes personal data on behalf of the data controller. While they carry out the processing activities, they do not decide on the why and how of processing but follow the data controller's instructions.

If you are using third-party services in your app such as cloud hosting or advertisement or analytics tools, these often act as data processors. They handle the data as instructed but do not decide on the overall purpose or means of that processing. As app owner, when you engage with third-party services that process end-user data on your behalf, it is crucial they have robust data protection practices and that there is clear agreement about their role and responsibilities.

Data subject (or data owner)

A data subject is the identified or identifiable person to whom the personal data relates. It is essentially the individual whose data is being processed.

Every end user of your mobile app is a potential data subject. Their rights, as defined by data protection regulations, include being informed about how their data is used (often via a privacy policy), accessing the data held about them, requesting corrections to that data and requesting the data be deleted. It is crucial to build features and processes in your app that respect these rights.

When the mobile app is made available to the end user and it collects and processes their personal data (starting with registration data, for example), the key parties in the app ecosystem assume certain data protection roles. The general obligations can be summarized (see table 8.4), though each jurisdiction will have its own specific list.

Table 8.1 Key parties, data protection and obligations

Key party	Data protection role	Obligations

App owner	Data controller	Ensure the mobile app does not collect unnecessary personal data. Implement strong security measures to protect end-user data. Perform regular security. In cases of sensitive data processing and/or use of new technologies such as AI, perform a data protection impact assessment (DPIA).[(a)] Provide transparent information about data processing in the mobile app. Comply with app store information and security requirements. Allow end users to access, modify and delete their personal data. Handle data breaches appropriately, including notifying affected users in accordance with applicable data protection laws.
App stores	Data controller	Ensure the distributed mobile apps comply with data protection laws. Perform regular security and, in cases of sensitive data processing and/or use of new technologies such as AI, perform a DPIA. Ensure clear privacy policies are in place and accessible to end users. Check data protection measures of the mobile app distributed. Manage end-user complaints related to data protection issues. Inform end users of updates or changes in data processing activities. Handle data breaches appropriately, including notifying affected end users.
Service providers	Data processor	Ensure services/products comply with data protection laws.

		Offer transparency on data collected and processed. Implement strong security measures to protect data. Allow app owner to access, modify and delete data when necessary. Inform the app owner of any changes to data handling processes. Handle data breaches appropriately and notify the app owner.

[a] More information on when a DPIA may be legally required is available on the WIPO website, https://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo-guide-data-protection-mobile-apps.pdf.

Source: the authors.

Data subjects (end users and their families) have significant rights under privacy legislation, the most important, from a compliance point of view, being the right to be informed about data processing, including the data being processed, and for what, how and by who. Rights also include access to and rectification of any incorrect data, and the right not to be subject to unnecessary or unjustified processing (and, accordingly, to object to or request such processing cease). App owners must publish their privacy policy with the mobile app, including this information as well as legal information about the owner and how to contact them. App stores require this policy to be made expressly available.

More information on the data protection obligations involved in each role, and issues that impact the development and use of mobile apps, are available in the WIPO Guide to Data Protection in Mobile Applications, online at www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo-guide-data-protection-mobile-apps.pdf.

8.4. Main risks and issues

The complexity of mobile app data flows magnify the personal data protection implications, given the multitude of ways in which data can be compromised.

The European Union Agency for Cybersecurity (ENISA) has indicated that three of the main risks with mobile apps derive from the following:[40]

1. **Integration of software into user's private mobile (handheld) device**: this implies much personal and/or sensitive data is collected, given devices are usually always on and include identifiers such as device ID, metadata and geolocation data that can allow tracking of the device or its users. Further, the mobile nature means they are susceptible to vulnerabilities because they have user interfaces limited by the small screen, which can make information less accessible to users.
2. **Complexity of dataflows**: the number of players involved in developing and deploying mobile apps (app owners and publishers, and service providers, for example), and the fact app owners rely on these parties to deliver their apps to end users.
3. **New technologies such as AI**: the integration of AI into mobile apps (AI-infused mobile apps) has exciting prospects, from improved end-user experience to increased operational efficiency, but these advanced tools come with risks, such as algorithmic bias, where AI systems may unintentionally perpetuate/amplify existing social prejudices based on biased or incomplete training data. Such algorithms may result in unfair or discriminatory outcomes affecting minority groups or marginalized individuals. Beyond ethical concerns, we should mention risks related to data privacy, given AI models often require access to large amounts of data, increasing the potential for misuse or breach, since AI use may expose the app to new vulnerabilities or potential security threats.

[40] European Union Agency for Network and Information Security. *Privacy and Data Protection in Mobile Applications*. ENISA, 2018. <www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications>.

Security must be integral throughout the life cycle of an app; while the development phase is crucial, there are also risks that can affect security when downloading and using mobile apps. Malicious mobile apps continue to make it on to app stores, showing that many store review processes are not sufficient. Meanwhile, app owners with no malicious intent may be publishing apps that do not adhere to security and data protection best practice because many app stores place the onus on owners to find this information for themselves, and some are failing to impose robust vetting procedures or provide security or privacy requirements altogether.

Incorporating security measures at this stage is akin to setting the foundation for a building; if the foundation is weak, the entire structure is vulnerable. Addressing security during the development process not only ensures the mobile app is equipped to handle potential threats but also reduces the cost and complexity of dealing with vulnerabilities in the later stages. By embracing a privacy-by-design approach, developers can ensure that privacy and data protection are at the forefront, fostering trust among users and stakeholders, and paving the way for a safer digital landscape for all.

The following (see table 8.5) are some of the most common privacy and security risks that may occur in developing the mobile app and in the subsequent stages of its life cycle, along with some examples and preventive measures.

Table 8.2 Common privacy and security risks

Risk/issue	Example	Preventive measure
Inadequate data encryption: a principal risk in mobile app development is the lack of proper encryption. Without secure encryption algorithms, data transferred between a user's device and backend servers can be intercepted and compromised.	Consider a banking app that does not employ strong encryption protocols. Malicious actors could easily intercept sensitive transactions and steal a user's financial information.	Implement industry-standard encryption algorithms and update them regularly.

Insufficient authentication and authorization: a mobile app that does not require strong authentication mechanisms exposes its users to potential breaches.	A health mobile app without multi-factor authentication could be accessed by unauthorized users, risking the exposure of private medical information.	Integrate multi-factor authentication and robust authorization mechanisms.
Improper storage of sensitive data: mobile apps often store data on the device. If this is not securely stored, it can be extracted by malicious software.	A fitness tracking mobile app that collects more data than it discloses (e.g., heart rate, sleeping patterns) and sells it to third-party advertisers without user consent.	Ensure data stored on the device is encrypted and provide options for secure cloud storage.
Third-party libraries and SDKs: vulnerabilities arise due to poor coding practices. These can be exploited through methods like SQL injection, where attackers can access a database by inputting malicious code.	An e-commerce mobile app with vulnerable code could allow attackers to bypass security measures, potentially accessing user payment details.	Vet and monitor third-party software. Regularly update libraries and SDKs to the latest secure versions.
Inadequate testing and quality assurance: if mobile apps are not tested rigorously for potential security threats, vulnerabilities can go unnoticed.	A photo-sharing mobile app that has not been tested for security might unintentionally expose a user's private photos to unintended viewers/the public.	Establish thorough testing and quality assurance (QA) processes, including penetration testing and vulnerability assessments.
AI vulnerabilities: with the integration of AI into mobile apps, there is a potential risk of adversarial attacks where attackers feed deceptive data into the AI system to fool it.	An AI-powered facial recognition mobile app could be tricked into misidentifying a user, granting access to an imposter.	Incorporate adversarial training, validate AI models rigorously, and keep AI systems updated.
Lack of regular updates: failing to push regular security updates make an app susceptible to known vulnerabilities.	A popular social media mobile app that does not regularly update its security protocols might be vulnerable to a breach,	Maintain a schedule for regular security updates, and push them to users promptly.

	compromising millions of user accounts.	

Source: the authors.

Take a moment to go through the following checklist. App owners should ensure they follow best practices to mitigate potential security risks in mobile app development.

Checklist: security measures

1. Data storage and handling

☐ Ensure secure storage of sensitive data; for example, using encryption.

☐ Avoid storing sensitive data unnecessarily. Discard what is not needed.

☐ Ensure data backups are encrypted and securely stored.

2. Data communication

☐ Encrypt data transmitted over networks; for example, using secure sockets layer (SSL)/ transport layer security (TLS).

☐ Implement certificate pinning to prevent man-in-the-middle attacks.

3. Code security

☐ Conduct regular code reviews for potential vulnerabilities.

☐ Use code obfuscation to prevent reverse engineering.

☐ Avoid hardcoding sensitive data; for example, API keys.

4. Authentication and authorization

☐ Implement strong authentication mechanisms; for example, multi-factor authentication.

☐ Ensure proper role-based access controls.

☐ Manage user sessions properly; for example, timeout, invalidation.

5. Information exposure

☐ Limit information in error messages to prevent data leakage.

☐ Avoid logging sensitive information.

6. Third-party components

☐ Vet third-party libraries or SDKs for known vulnerabilities.

☐ Regularly update libraries and SDKs to their latest secure versions.

7. Cryptography

☐ Use strong encryption algorithms and methods.

☐ Regularly rotate encryption keys and store them securely.

8. Web views

☐ Sanitize data displayed in web views to prevent cross-site scripting (XSS) attacks.

☐ Limit the functionalities of web views to necessary actions only.

9. Binary protections

☐ Implement binary protections to prevent tampering.

☐ Ensure mobile apps have mechanisms against code injection.

10. Platform and OS

☐ Regularly update the mobile app for compatibility with latest OS security features.

☐ Do not solely rely on the mobile app's security. Implement app-level security measures.

11. Testing

☐ Regularly conduct vulnerability assessments.

☐ Undertake penetration testing to uncover potential security loopholes.

☐ Address identified vulnerabilities before mobile app release.

12. Physical threats

☐ Implement security features for stolen or lost devices; for example, remote wipe or lock.

☐ Ensure on-device data is encrypted.

13. Stay updated

☐ Remain informed about the latest threats and vulnerabilities in the mobile landscape.

☐ Join developer forums or groups that discuss mobile app security.

14. General best practices

☐ Educate your development team on the importance of protecting personal data.

☐ Document all security practices and keep them updated.

8.5. Privacy by design and by default

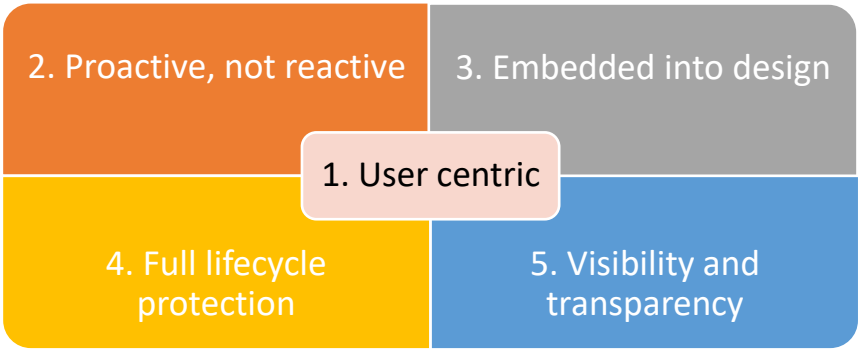
Privacy by design and privacy by default are two foundational principles that can guide mobile app owners in creating secure, trustworthy applications that respect end user data protection rights. This section briefly presents these concepts, clarifying their importance and offering practical guidelines for implementation.

8.5.1. What is privacy by design?

Privacy by design (PbD) is a proactive approach to privacy. It suggests that privacy and data protection measures should be embedded directly into the design specifications of technologies, practices and operations. Instead of being an afterthought, data protection should be a primary goal from the beginning.

The concept of PbD, initially developed by the Ontario Information and Privacy Commissioner, Ann Cavoukian, and first mentioned in 2009, has gained traction over the years. It has been incorporated into various standards and regulations, the most notable being the European Union's GDPR. Adopting PbD can help organizations meet regulatory requirements, foster trust with customers, and mitigate risks associated with data breaches or other privacy-related incidents.

Figure 8.4 - Privacy by Design principles



Source: the authors

To build PbD into mobile apps, it is important to understand the five main principles in more detail:

1. **User centric**: the need to put users at the forefront of data protection considerations. This means being open with users and letting them know who is collecting and using their personal data, why it is being used, and what is being shared and with whom and for what purpose.
2. **Proactive not reactive**: address data protection concerns before they become issues, rather than addressing breaches after they occur.
3. **Embedded into design**: recognize that users have privacy interests, which means they have their own expectations, needs, wants and concerns that must be addressed in a proactive manner from the start rather than as an add-on or afterthought.
4. **Full life cycle protection**: personal data should be securely protected throughout its entire life cycle within the app.

5. **Visibility and transparency**: design components should operate according to principles that are openly vetted and verified by users. App owners and other key players should be assured that business practices and technologies are functioning in a manner consistent with data protection values.

Case study: MovieNight, from reviews to unneeded cinema locator

Background

MovieNight is a mobile app that enables end users to search for movies, read reviews and create watchlists. An unnecessary feature has recently been introduced, where users can see nearby cinemas, though most of the app's functions are not dependent on location.

Scenario

John decides to download MovieNight to discover new movies and build his watchlist. He is excited to explore its features but is immediately met with a location access request.

Steps

1. Immediate access: after installing and opening the app, but before getting to the home screen or registration process, John is presented with a request: "MovieNight wants to access your location."
2. Lack of information: the request does not explain why the location is needed, nor does it assure John that his data will be kept private or describe how it will be used.
3. End-user action: if John clicks Allow, the app gains access to his location. There is a subtle icon showing cinemas on the home screen, but it is not prominent, and John might not notice or use it. If John clicks Don't allow, he can still use the mobile app but an annoying and persistent banner appears at the bottom of his screen prompting him to enable location services for the 'full experience'.
4. Hidden motives: deep within the mobile app's settings, under a generic Data use section (not clearly marked as data protection/privacy-related), there is a brief mention that user location data may be shared with third-party advertisers for targeted advertising, including movies being released nearby.

5. No control: John decides he no longer wants the app to access his location, but there is no easy toggle in the settings. He has to go to his phone's system settings to revoke location access, a process that many users might not be familiar with.

Conclusion

MovieNight showcases several bad practices related to data protection:

- Unnecessary/unjustified processing: the app must not access a user's location if the app is not a location-based service app. As the location data is secondary to the app and is needed in order to meet other commercial purposes, MovieNight needs to get the user's active consent.
- Ambiguous consent: the mobile app does not clearly explain why it needs location access.
- Misleading features: the cinema feature is not a primary function and seems more like an excuse to gather user location.
- Lack of transparency: the app hides its true motive of sharing data with third-party advertisers and does not give users easy control over their data.

8.5.2. What is privacy by default?

The data protection principle, privacy by default (PbDft), suggests that systems, services and products should ensure the highest level of user privacy as their standard setting. In other words, when a user acquires a new product, signs up for a new service or uses a new system, the default configurations should be the most privacy-friendly ones.

Figure 8.5 Privacy by default concepts

Source: the authors.

It is important to understand in more detail the for main concepts of privacy by default:

1. **Minimum data collection**: mobile apps should collect only the minimum amount of user data necessary for the app to function correctly. If an app function can work without a specific piece of data, it should not ask for it. When developing a mobile app, always prioritize user data protection rights. Never secretly gather personal information. Always be transparent and inform end users upfront about what data you are collecting and how it will be used.
2. **Limited data retention**: data should not be kept indefinitely. There should be clear retention policies indicating how long it is retained and when it is deleted. If you are storing data that is tied to a unique user via cookies or device identifiers, even if you strip out other personally identifiable information, it is not truly anonymous. A safer bet is to completely remove or hash that unique identifier. That way, you are moving closer to genuine anonymity.
3. **Limited data access**: mobile apps should not request access to user data or device functions that are not essential for the app's primary functionality. When accessing end user contact list data for specific mobile app functionalities, ensure you gather only the fields required for that purpose. It is imperative not to divert or repurpose this data for any additional purposes unless the user has explicitly provided consent. Uphold user trust by maintaining data integrity and transparency.
4. **High default settings**: instead of automatically enrolling users in data collection processes and requiring them to opt out, a privacy by default approach will require users to actively choose to opt in. Regarding the social media app's development, when the default privacy setting for an account is configured to 'public', it is vital to clearly inform end users prior to the collection of any personal data or initiation of the account setup process. End users must be provided with a clear and unambiguous option to consent or decline.

Case study: MobiFit, a health tracking mobile app

Background

MobiFit is a mobile app that aims to help users track their daily steps and calories burned, and set exercise goals. Given increasing concerns about user privacy, MobiFit's app owner opted to follow the privacy by default principles.

1. Minimum data collection

Scenario: a user, Alice, downloads and installs the MobiFit app.

Implementation: on setup, MobiFit asks Alice to enter her age, weight and height to calculate burned calories. Additional details such as address, contacts or social media accounts are not requested as they are not necessary for the app's core functionalities.

2. Limited data retention

Scenario: Alice has been using the MobiFit mobile app for a year.

Implementation: MobiFit's policy states that user data related to daily steps and calories is retained for 90 days, after which it is automatically deleted. This ensures Alice's historical data is not stored indefinitely. When she checks her history, she sees only the last months of data.

3. Limited data access

Scenario: Alice notices the app has a feature to send reminders.

Implementation: MobiFit wants to send notifications to remind Alice to complete her daily step goal. When she enables this feature, the app requests permission to send notifications but does not request access to other device functionalities such as camera, contacts or microphone, as they are irrelevant to its primary functionality.

4. High default settings

Scenario: MobiFit introduces a new feature to share daily achievements on social media platforms.

Implementation: by default, this feature is turned off. When Alice opens her app, she receives a prompt explaining the new feature and is asked if she would like to opt in. If she chooses not to, the app will not share anything. Alice's active consent is required to activate this feature, ensuring she is not automatically enrolled.

Outcome

By adhering to the privacy by default principles, MobiFit ensures it respects and protects the user's privacy, builds trust among its user base, and stands out in the market for its strong privacy standards.

Advantages of implementing privacy by design and default in a mobile app's life cycle

1. Builds trust: by respecting user data protection rights from the onset, businesses can build trust with their users. This can improve user retention and loyalty.

2. Reduces risks: by being proactive and ensuring high standards of data protection, businesses can mitigate the risks of data breaches and the associated reputational and financial damages.

3. Regulatory compliance: with data protection laws like the GDPR in the European Union, adhering to privacy by design and by default principles can help in regulatory compliance, thus avoiding potential fines.

4. Competitive advantage: as users become more data protection-conscious, having robust security measures can be a unique selling point for mobile apps.

5. Enhanced user experience: when users know that minimal data is being collected and their privacy is prioritized, they are more likely to have a positive experience and less likely to be concerned about sharing necessary information.

6. Efficient data management: collecting only essential data means there is less data to manage, store and secure. This can lead to cost savings and performance improvements.

Privacy by design and by default are not just principles to adhere to for legal or compliance reasons. They represent a mindset that places the user at the center of the product design process. For mobile app owners, integrating these principles can offer not only a competitive advantage but also a sustainable, user-centric model of business.

Privacy Checklist

The general data protection issues that should be taken into account when developing an app include:

1. **Understand the regulatory landscape**: before beginning coding, familiarize yourself with the data protection regulations that apply to your target audience.

2. **Data minimization**: collect only data that is essential for the app's functionality. Avoid hoarding unnecessary information as this increases risk and potential liability.

3. Encryption:

- Data at rest: ensure all stored data, whether on local devices or cloud storage, is encrypted, thus making it unreadable without the corresponding decryption key.

- Data in transit: utilize protocols such as TLS to ensure data transferred between the app and servers is encrypted and secured from potential eavesdroppers.

4. **Regularly update and patch**: ensure all parts of your application, including third-party libraries and backend servers, are regularly updated to protect against known vulnerabilities.

5. **Secure authentication**: use strong password requirements, multifactor authentication and technologies such as OAuth to ensure only authorized users can access accounts.

6. **Access controls**: ensure users can access only the data they are supposed to. Utilize role-based access controls (RBAC) if needed, especially in multiuser applications.

7. **Secure coding practices**: protect against common threats such as the common attack vector SQL injection, cross-site scripting (XSS) and cross-site request forgery (CSRF) by following secure coding best practices.

8. **Transparency with users**: always maintain a clear and concise privacy policy that explains

- what data you collect;

- why you collect it;

- how long you retain it; and

- with whom you might share it.

9. **Data retention policy**: implement and communicate clear data retention policies. Delete user data when it is no longer necessary for the service or after a user's account is terminated.

10. **Incident response plan**: have a plan in place to respond to any data breaches. This includes identifying the breach, notifying affected users and taking corrective action.

11. **Regular audits**: conduct regular security audits to identify vulnerabilities, including automated scans and manual code reviews.

12. **Third-party vendors**: if your application relies on third-party vendors, ensure they adhere to robust security practices and data protection regulations. If they process the personal data on your behalf, make sure that you sign a data processing agreement that regulates the obligations and responsibilities.

13. **Data backup**: regularly back up user data in a secure manner. In the event of data loss, having encrypted backups can be crucial for restoration and trust.

14. **Right to be forgotten**: ensure your systems allow for easy deletion of user data should they request it, in accordance with regulations such as the GDPR.

15. **Data portability**: users should be able to obtain and use their data for their own purposes across different services. Make sure you provide a way for users to download their data in a readable format.

8.6. Conclusions

This chapter outlines the intricate world of data protection in the mobile app space, shedding light on its importance, risks associated with its neglect and the significance of implementing adequate compliance and security measures. The essence of safeguarding personal data does not merely revolve around privacy principles but also involves the technical aspects of securing data from potential breaches and external threats. From the context and legal framework to the main risks and challenges, it gives an overview of what app owners must be aware of in terms of data protection.

The principles of privacy by design and by default are crucial concepts, and app owners and developers or agencies are urged to incorporate privacy compliant measures from the app's conception. With an ever-increasing volume of sensitive data, and the integration of new technologies such as AI, it is imperative that app owners prioritize

users' privacy and security, are diligent in processing personal data and adopt robust security measures.

Privacy and security are not just regulatory requirements but critical legal and ethical standards that can make or break an app's reputation and trustworthiness in the market.

Key takeaways for privacy and mobile apps

- All mobile apps process personal data to some extent.
- With more and more privacy regulations worldwide, app owners in particular must understand their data protection obligations.
- Perform an analysis of the personal data flow, and the different roles and responsibilities that derive from it.
- Pay attention when processing sensitive personal data and put the necessary safeguards in place.
- Correctly implementing the necessary security measures guarantees the protection of personal data.
- Apply privacy by design and by default principles from the beginning of app development or ensure they are implemented by the contracted developers and/or agencies.
- Make sure controls are in place to ensure compliance with data protection principles throughout the app's life cycle.

8.7. Useful links and resources

WIPO, A *Guide to Data Protection in Mobile Applications*. Wipo.int. 2021. <https://www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo-guide-data-protection-mobile-apps.pdf>

European Union Agency for Cybersecurity, *Privacy and Data Protection in Mobile Applications*. 2018. <http://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications>

European Data Protection Supervisor, *Guidelines on the Protection of Personal Data Processed by Mobile Applications provided by European Union Institutions*. 2016. <https://www.edps.europa.eu/sites/default/files/publication/16-11-07_guidelines_mobile_apps_en.pdf>

GSMA, *Privacy Design Guidelines for Mobile Application Development*. wwwgsma.com. 2018 https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2018/02/GSMA-Privacy-Design-Guidelines-for-Mobile-Application-Development.pdf

Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)*. 2022. Online at <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf>

RPC, *Changes to data protection legislation in Asia – 2022 update (including Mainland China*). rpc.co.uk. Visited March 2024 <https://www.rpc.co.uk/perspectives/data-and-privacy/changes-to-data-protection-legislation-in-asia-2022-update-including-mainland-china/>

Hogan Lovells, Asia-*Pacific Data Protection and Cyber Security Guide 2022*. 2022. https://f.datasrvr.com/fr1/022/16167/APAC_Data_Protection_and_Cyber_Security_Guide_2022.pdf

Fernandez, D., Barbero, J. *Road to homogenization? Argentina publishes a new bill to replace the Personal Data Protection Law*. Int. Cybersecur. Law Rev. 4, 471–487 (2023). https://doi.org/10.1365/s43439-023-00098-7

Chapter 9. Open source and mobile apps

9.1. Introduction

This chapter provides an overview of IP and open source in relation to development and licensing of mobile apps. In particular, it focuses on what is open source software and licensing, and the key issue of ensuring compliance with open source licenses on components embedded in apps. We look at how to engage with the open source community, as important providers of relevant technologies for apps, and the relationship between open source licenses and app stores.

Much of the software currently under development globally, including tools, components, frameworks and database management software, is open source, to such an extent that most new software cannot be developed without open source elements. We will help the reader to better understand open source licensing within the app sector and the management of open source components with the technology infrastructure and building blocks of the app, and even how to free their apps or technologies as open source to take advantage of the benefits of this licensing model.

Open source numbers

A high-level search on GitHub for mobile apps reveals 107,000 relevant projects. A user at GitHub, LinuxCafeFederation, has published a list of more than 200 off-the-shelf apps for Android. A search for 'mobile' on SourceForge, an older yet still valuable open source repository, reveals 5,555 results. This understates the amount of open source software that is used in mobile application solutions, given a significant quantity of general purpose open source software is relevant for backend servers, data management, databases, security, connectivity and the like.

More information on open source is available in the WIPO guide on "Open Source for Mobile Apps, online at www.wipo.int/export/sites/www/ip-development/en/agenda/docs/wipo-tool-open-source.pdf.

9.2. The importance of understanding open source licensing

Open source code, together with free software, encompasses software that is freely accessible for use, modification and distribution by anyone. This characteristic facilitates a collaborative environment where companies can collectively bear the burden of developing technologies.

A substantial portion of software being developed worldwide falls under the open source category, to the extent that it has become a fundamental aspect in the creation of new software projects. Its influence is all-encompassing, reaching from budget-friendly consumer devices to the world's most powerful supercomputers. Notably, every Android mobile device relies on an open source operating system, and open source extends to a significant portion of the Internet's infrastructure, emphasizing its critical role in the modern technological landscape.

The appeal for companies is clear. There is plenty of high-quality, widely respected software accessible, free of charge with minimal restrictions, and ready to use.

Examples: open source solutions for building apps

Flutter

Flutter is an open source framework created by Google for building mobile, desktop and web apps from a single codebase. It was released in 2017 and gained popularity due to its ease of use and performance capabilities. Flutter's code is open source, distributed under the BSD 3-clause license**Error! Hyperlink reference not valid..**

Apache Cordova

Formerly known as PhoneGap, Apache Cordova is an open source mobile application development framework. It enables the creation of apps that run on multiple operative systems, such as iOS, Android and Windows. Apache Cordova offers a set of plug-ins that allow access to device features, such as battery status, camera and geolocation. Its code is distributed under the Apache 2.0 license.

Ionic Framework

Ionic Framework is an open source, front-end user interface (UI) framework for building cross-platform mobile and web apps. It provides a set of predesigned UI components (such as buttons, tabs and cards) that are easily customized and responsive across different devices. Ionic Framework's code is distributed under the MIT license.

However, open source software, while free, still requires careful usage due to licensing conditions. Violating such conditions can lead to legal consequences, and for this reason attention must be paid to identifying and complying with them. In fact, while meeting typical license requirements, such as retaining copyright notices, is manageable, compliance with more complex obligations, including providing source code and licensing it accordingly, can be challenging. Further, issues with license compatibility may arise when combining components with different types of open source licenses.

Software developers, including app developers, must have a process to identify open source code in their apps and ensure compliance with licenses. Before using an open source component, it is crucial to verify that it is available under a license that enables use in the way envisaged by the developer. This is part of the so-called compliance process illustrated in this chapter.

The following sections will provide insight into the main concept of open source, to put the above in context. Open licensing is not limited to software, and there are also open licenses for data and, more popularly, for content (see section 8).

9.3. Main concepts of open source: open and free software licenses

Open source software refers to software distributed under licenses allowing unrestricted use, modification and distribution, with access to source code. These licenses may include conditions such as retaining attribution notices, disclaimers, notice files and

copies of the license text during distribution. Sometimes, additional requirements demand the availability of source code, including that of any linked software, to recipients under the same license terms. In essence, open source software complies with the definition provided by the Open Source Initiative (OSI).[41]

Both the OSI and the Free Software Foundation are organizations dedicated to promoting and advocating the principles of free and open source software. Legally, there is little distinction between open source and free software. It is worth noting that from a compliance standpoint, distinguishing between the two has little impact because the ultimate goal is to adhere to the licensing terms of the relevant software component.

Open source licenses can be divided into two main categories, namely permissive and copyleft.

9.3.1. Permissive licenses

Permissive licenses are a type of open source licenses with minimal restrictions: they allow the integration of the licensed component into any code. Both the component and the software solution embedding the component can be redistributed under any license, including proprietary licenses.[42]

Examples: permissive licenses

MIT

The MIT license is a simple, short license that allows all uses, copies, modification, mergers, publications, distribution, sublicensing and sale of copies of the component with no restriction. It requires that a copy of the copyright notice and of the license

[41] Open Source Initiative. "The Open Source Definition." *opensource.org*. July 7, 2006. <*www.opensource.org/osd/*>.

[42] Proprietary licenses are a type of software license that restrict or prevent the modification and distribution of the software. Unlike open source licenses, they do not grant access to the software's source code.

itself is included when the component, or a software program embedding the component, is distributed.

Apache 2.0

The Apache license, version 2.0 is a more detailed and comprehensive license than the MIT. While the allowances and the obligations are the same, the Apache 2.0 includes a patent grant clause, enabling users to access the necessary patents required for utilizing the component in compliance with the license terms.

BSD 3-clause

The 3-clause BSD license, in addition to the allowances and obligations in the MIT license, includes a clause preventing users from including the names of software contributors and/or copyright holders to endorse or promote the products derived from using the open source component without prior written permission.

9.3.2. Copyleft licenses

Unlike permissive licenses, copyleft licenses impose additional obligations on redistribution of the open source component and, in certain circumstances, of the whole software or app code. They require that if derivative works of a component are distributed, each derivative work must be licensed under the same terms as the original work (or, sometimes, a different specified license). A copy of the source code to the derivative work must also be made available on its distribution.

The category of copyleft licenses can be divided into three subcategories:

1. Strong copyleft refers to those open source licenses that require derivative works or modifications of the original code to be distributed under the same copyleft license (or a compatible one). For example, the GNU GPL license.

2. Weak copyleft licenses require the original code, and any modifications made to it, to remain under the same license and provide access to the source code. In this case, the copyleft effect applies only to the component distributed under the weak copyleft license, not to the whole software or app embedding the weak copyleft component. For example, the GNU LGPL license or the Mozilla Public License.
3. Cloud copyleft licenses address the use of software in cloud computing, where the component is not distributed as such. The copyleft effect applies when the applicable component is part of the server-side code and its functionality is made available over a network, for instance, in a software as a service (SaaS). For example, the GNU Affero GPL license.

Examples: copyleft licenses

Strong copyleft: GNU GPL 3.0

The GNU General Public License, version 3 is the most recent version of the GPL license. Comprehensive and clear, it covers various scenarios such as the distribution of verbatim copies and modified copies. With every distribution of the work, modified versions of the work or works that are based on it, you have to include the copyright notice, notices stating the GPL 3.0 license applies to the code (i.e. maintain the same license) and that all warranties are disclaimed, and a copy of the license and access to or an offer to provide the source code. With any modifications of the code, the work must carry prominent notices stating it has been modified and the relevant date.

Weak copyleft: GNU LGPL 2.1

The GNU Lesser General Public License, version 2.1 is widely used and designed primarily for software libraries. It requires that the source code of the library distributed under the LGPL 2.1 license and any modifications thereto are made available to recipients, while the larger software that uses the LGPL 2.1 (e.g. as a software library) can be distributed under any license.

Cloud copyleft: GNU Affero GPL 3.0 (AGPL)

GNU Affero General Public License, version 3 is based on the GNU GPL, with an additional requirement to ensure that users interacting with the software over a network

have to be offered access to the corresponding source code under the same AGPLv3 license. Like the GPL, the AGPL demands that if you create a larger software program that includes AGPL-licensed code, and this is made available to third parties, then the entire program must also be licensed under the AGPL, and the corresponding source code must be made available to the licensee.

For the different categories of license, see table 9.1.

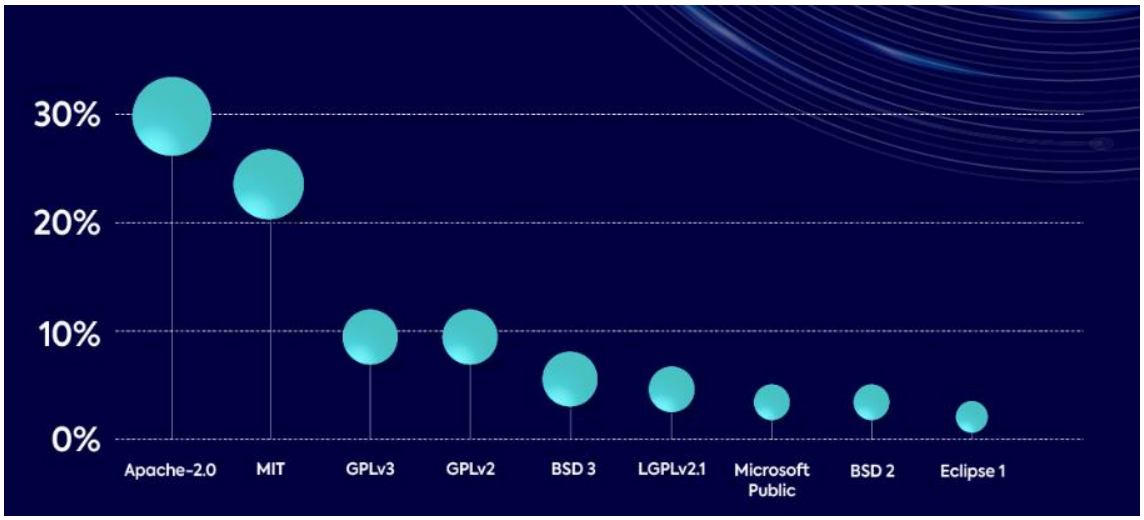
Table 9.1 Open source licenses, categories

Type	Characteristic	Licenses	Examples
Permissive	No restrictions on reuse/redistribution. Derivative works and compilations can be closed/proprietary.	BSD, MIT, Apache 2.0	Android, Apache web server, Open Stack, PHP, Ruby
Weak copyleft	Copyleft applies on the original core code only and direct derivative works, but not on extensions or composed works using the code.	LGPL, MPL, CPL	JBoss, Mozilla, LibreOffice, Joomla
Strong copyleft	Copyleft on all the redistributed work, including derivate works and composed works incorporating or otherwise based on the code.	GPL2, GPL3, EUPL	Linux, Asterisk, GIMP, MySQL, Drupal, MediaWiki
Cloud copyleft	Copyleft obligations as to licensing and providing source code also apply when the code is not distributed but its functionality is made available over a network.	AGPL, EUPL	Magenta, Grafana.

Source: the authors.

The most popular licenses in 2021, are indicated in figure 9.2.

Figure 9.1 Most popular open source licenses, 2021



Source: Mend.io, formerly WhiteSource. "The complete guide for open source licenses." *mend.oi*. 2022. <https://www.mend.io/wp-content/media/2021/01/The-Complete-Guide-for-Open-Source-Licenses-2022.pdf>.https://www.statista.com/statistics/1245643/worldwide-leading-open-source-licenses/

9.3.3. Non-open licenses

It should be noted that some licenses with similar characteristics to open source licenses do not meet the Open Source Definition (as identified by the OSI) and, therefore, cannot be considered open source. Examples of non-open licenses include: (1) noncommercial license that restricts the field of use of the component, (2) no derivatives license that prohibits creating derivative works clearly infringing the fundamental freedoms of open source licenses, (3) freeware license, which consists of proprietary licenses with no fees associated, and (4) source-available license that provides access to the source code of the software, while imposing restrictions on its use, modification and/or distribution.

9.4. Pros and cons of open source

There are advantages and inconveniences to choosing open source as a licensing regime. In most instances, the value of using open source technologies or going open yourself depends on the technology involved, the business model and the potential community of stakeholders and participants.

On the one hand, open source technologies can be mature, stable and supported by a big community, such as the Apache, Android or Linux kernel communities. These make significant technologies available to all for free and under open licensing terms, so the technologies can be used, adapted, embedded in apps and the online servers, and (re)distributed to users: no lengthy negotiations on licensing terms, no royalties and very few, if any, restrictions. On the other hand, there is also a large number of immature or non-supported open source projects that offer little in the way of security, sustainability and long-term existence. The transparent nature of open source, however, means developers who are thinking of using a component, framework or other open technology can see the dynamics of a project online, evaluate the quality and security in terms of published issues and corrections, and have a view as to its value.

There are several considerations to take into account: there is often no guarantee that the project will continue ‘next year’, or that bugs will be fixed, and corrections made (although you do have the source code to sort them yourself). But there are ways to mitigate this, as many relevant projects are often supported by a company that provides such fixing, and expertise and professional services around the technology, as well as offering proprietary extensions or adaptations that may be a better fit for the app developer or owner.

Releasing software under an open source license within a public repository such as GitHub, GitLab or BitBucket enables third parties to access and use the code and to give back to the project, with contributions that go from bug warnings (issues) to sending fixes for the bugs/errors or providing new evolutions to the software. This creates a community of experts around the software, on a potentially worldwide level, which can help dissemination and uptake, and some open source technologies such as JSON have become a de facto standard. One measure of project success is the number of downloads but more relevant is the number of contributors and contributions. For popular projects, this has led to faster and better corrective maintenance, new versions with more

features (or fewer features, to be more efficient or work faster), thus increasing the quality and relevance of the work, though of course, this does not happen for all open source projects.

In terms of quality and IP, there is no general guarantee or contractual warranty in an open source license that the software operates correctly or conforms to its documentation, or that it does not infringe any third-party IP rights, whether patent or copyright. While some proprietary licenses also disclaim such guarantees, most commercially supported software comes with warranties of conformance and correct operation and an indemnity against third-party IP claims. However, many open source projects have been around for years without any IP claims, and the frequent updates and new versions reveal a high degree of quality. Further, there are companies whose business model is to provide commercial grade warranties on open technologies to paying clients.

Example

One difference between using a version of the GNU/Linux open source operating system under the GPLv2 license (for example, Fedora Linux) and acquiring an enterprise license for, basically, the same software (for example, Red Hat, Canonical or Suse Enterprise licenses), is the set of commercial grade warranties offered by the licensor company. Other entities offer professional services for support on open source.

In terms of IP management, using open source components is fairly straightforward, though you do need to get to know the licenses to understand the implications. This contrasts with the nearly universal requirement to seek legal advice in relation to commercially offered (and negotiated) licensing terms, especially for core or customized technologies.

So, even if incorporating open source components into software code is a straightforward process, there are different factors that must be considered, from a technical, organization and legal point of view. Among these, the most relevant are the

component's performance and reputation, security and the existence of a community that keeps it updated, and compliance with the component's license.

9.5. Managing open source in mobile app development: licensing compliance

Open source is not public domain,[43] and its use must be managed, especially for distributed app technologies. The principal license obligations are presented, and how app developers and owners must be compliant with notice requirements, access to source code, and compatibility between components. We show how end-user agreements for mobile apps must also be compatible with open source licensing, and note the importance of ensuring that outsourced app developers assist the app owner in being compliant. There are standards such as Open Chain that support compliance.

As mentioned in section 2 of this chapter, the fact that open source components are available for free with wide exploitation rights does not mean they come without obligations. For this reason, compliance is a fundamental step when including open source software in the code of an app. The term compliance refers to the activities performed to ensure all obligations imposed by the licenses of the open source components used in a software or app are met.

Example: Ushahidi

Ushahidi is an open platform and app that enables situation awareness and empowers communities. It allows information to be collected, visualization and interactive mapping, with people able to submit through text messages, email or web form. Developed to provide information on violence in the post-electoral period in Kenya in 2007, it has since been deployed in several humanitarian crises, such as the 2010 Haiti earthquake and the Japanese tsunami in 2011. Ushahidi's platform is distributed

[43] Public domain refers to creative works not protected by copyright that are available for anyone to use, share, modify, distribute and publicly communicate, among other things, without restrictions or obligations.

under the AGPL version 3 license, which allows anyone to adapt the code to their needs, provided a copy is made available upon redistribution.

Compliance

Ushahidi reuses many open source components, and Ushahidi Platform at GitHub explains the licenses for software and libraries used in the program.

Specifically, what are the requirements for compliant use of open source software, and how do you meet them? The main obligations are outlined in table 9.2.

Table 9.2 Open source obligations and how to comply with them
Source: the authors.

Obligation	Obligation explanation	How to comply
Provide attribution	Almost all open source licenses require that copyright notices (© 2023 John Developer) and similar attributions be retained in source code, and that a copy is provided with the code if distributed in binary form.	How the attributions are delivered depends on the license and the mode of distribution, though in general: - include the set of attributions in the app's legal notices section; or - provide a persistent URL to a text file containing the attribution notices for a particular app release/version.
Maintain notices, license texts and disclaimers	Open source components might contain notice files that may, according to the applicable license, need to be preserved completely.	Include copy of the notices in the file with the attributions.
Source code (and offers to provide source code)	Copyleft licenses typically require that the source code to the relevant component be made available.	How the source code must be provided depends on the license. In general, it must be provided in an editable format (and you should not deliberately make it difficult to use): - Weak copyleft licenses: typically, source code is made available by supplying a persistent link. This link could lead to the GitHub or GitLab site where the underlying project is hosted (if the component has not been modified) or to your own repository (if the component has been modified). - GPL licenses: provide an offer, valid for three years, to provide the source code, or provide a download link.
License compatibility (inbound and outbound)	License compatibility means the license terms of all different components in a software distribution do not conflict (inbound compatibility), and with the terms of the license chosen to distribute the software/app (outbound compatibility).	If one license requires you to do something and another prohibits it (or makes it impossible to do), the licenses conflict and are not compatible. To ensure compatibility, an analysis of the licenses or the open source components and the license chosen to distribute the code of the app is necessary.

The software bill of materials

The obligations highlight the importance of maintaining a complete, accurate and up-to-date inventory of open source components used. The inventory of components is called a bill of materials, or software bill of materials (SBOM), while the compliance materials, which include notice files, license texts, attribution notices and disclaimers, are compliance artefacts. It is difficult to undertake any form of compliance exercise without a complete bill of materials, which is considered the starting point of any compliance exercise.

Checklist: generating and maintaining a SBOM

1. Keep a comprehensive list of all components as the app code is being developed. For each component, include:
   - name
   - source
   - version number
   - license.
2. Accompany the SBOM with a text file containing notice files, copyright notices, and relevant open source license text and disclaimers.
3. Update the SBOM every time a new version of the app is released.
4. If part of the app code is developed by external developers, require them to provide the necessary information with the components they included in their piece of code.

Hot tip: the standard format for defining a SBOM is SPDX.

Focus on compatibility

When two software licenses have conflicting requirements, they are considered incompatible, especially if combining the components triggers obligations under each license.

Compatibility must be determined (see table 9.2 above):

1. Among the licenses of the open source components embedded in the software of the app. This is called inbound compatibility.

2. With regard to the license chosen to distribute the app (choice of license is explained in section 6). This is called outbound compatibility.

Example

An app developer merged a component licensed under GPL 2.0 and another under EPL 1.0 into their mobile app's code. As these are both copyleft licenses – requiring the use of the same license on redistribution – the developer will be unable to comply with both licenses when distributing their app code. For this reason, the app's code cannot be distributed. However, internal use of the software is not affected, given copyleft obligations arise on distribution. To be able to distribute the app, the developer must solve the incompatibility issue.

How to determine when two (or more) licenses are compatible

There are different ways to determine compatibility:

1. Read the licenses, identify the obligations imposed by each and analyze whether it is possible to comply with all relevant obligations at the same time.

2. Seek advice from lawyers or consultants specializing in open source.

3. Look for tools and web pages that assist in identifying compatible and incompatible licenses, including:

- The European Commission's tool, the Joinup Licencing Assistant (JLA) Compatibility Checker, which helps with outbound compatibility.

- Free Software Foundation's GNU website has a section dedicated to listing open source licenses, describing them and identifying whether they are compatible with the GNU GPL license family.

Can license incompatibility be solved, and how? There are several ways to solve license incompatibility (see table 9.3 below), some easier to implement than others.

Table 9.3 Remedial measures for license incompatibility

Incompatibility remedy	Explanation	Comments
Multiple licenses	If a software component is available under multiple licenses, choose a license that does not create compatibility problems.	Not all software components are made available under more than a license. This remedial action might not always be feasible.
Replace or remove components	Review the software architecture and replace the problematic component with a compatible one or remove unnecessary components.	Not all components can be replaced or removed. This remedial action might not always be feasible.
Find equivalents	Look for components with equivalent functionality that have more permissive licenses.	Not all components have an equivalent that is permissive. This remedial action might not always be feasible.
Use different versions	Consider using a different version of the component if it is licensed under more permissive terms.	Not all software components have versions under different licensing terms. This remedial action might not always be feasible.
Contact copyright holders	Reach out to copyright holders to negotiate a specific license that resolves the incompatibility.	The copyright holder can be also contacted to ask for clarification on whether the obligations imposed by a specific license are triggered by the use made of the component.
Investigate component origins	Investigate whether the component being used is a modified version of another component under a more permissive license. If so, consider using the earlier component.	This may not always be the case, and therefore, this remedial action might not always be feasible.
Rewrite components	As a last resort, rewrite the problematic component from	This solution might imply changes in the software architecture. When doing so, take care not to copy the original

	scratch to ensure full ownership of the copyright.	code to avoid copyright infringement.

Source: the authors.

Checklist: use of open source for app owners and developers

1. Are you using third-party open source components?
2. Create a list of these components, with their URL, license name and version.
3. Store a copy of the license and the copyright notice.
4. View the license on the components and verify any copyleft effect (weak or strong) for compatibility with your outbound license or assignment to an app owner.
5. Scan the source code of the app in its final form to make sure there are no unknown or translative dependencies and include all results in the software list.
6. Create a SBOM for all included third-party open source components, which you can share with app publishers or online if you are releasing your app as open source software.
7. Include the SBOM with any distribution of the app code (source code or binary), together with all compliance information.
8. Review this checklist and update the SBOM for all new versions of the app code.

9.6. Licensing out the app

A fundamental part of every app's life cycle is the release and distribution of its first version, as well as all subsequent updates. App code, as all software code, is protected by copyright. Thus, third parties are allowed to use the code only if they are granted a license for it (see chapter 4 on IP protection). For this reason, choosing a license for the app code is a necessary step prior to its release and distribution – and extremely important given the chosen license will determine the different business models that can be adopted.

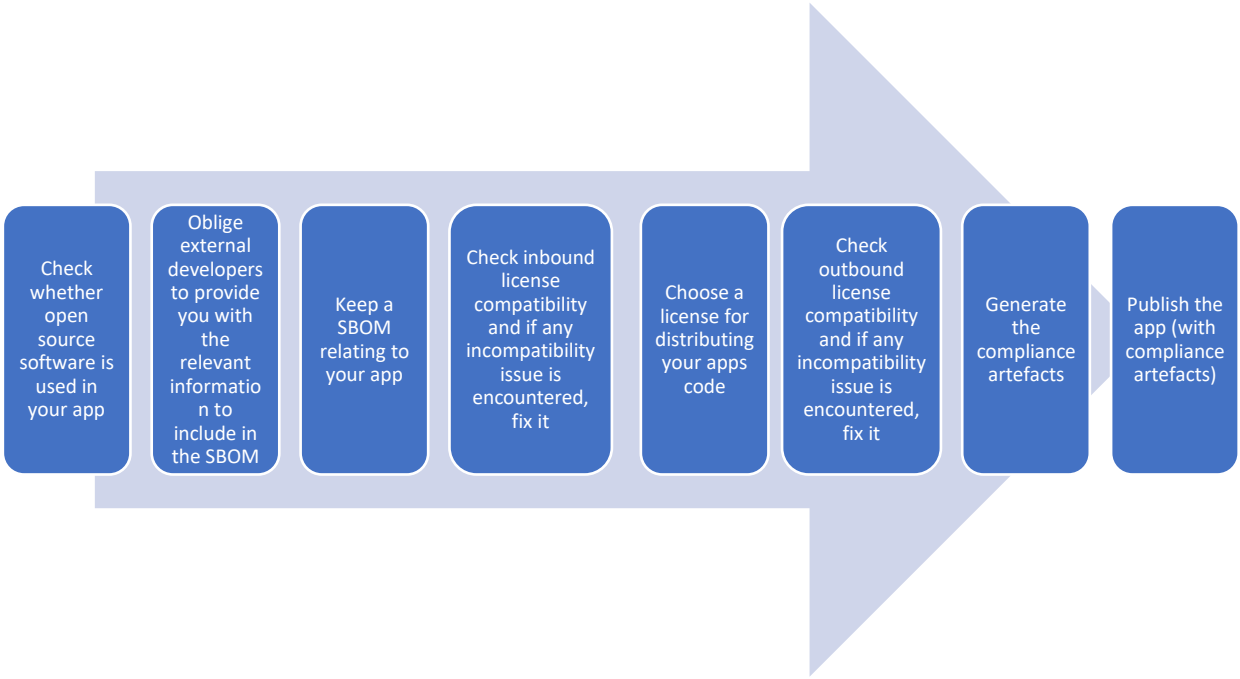
The choice of one license over another depends on several factors, including:

1. Compliance with requirements of the licenses over the software components used (outbound compatibility). If GPL code is included in the app, you may need to distribute the whole code under the GPL license.

2. Personal preference of the right holders.
3. Business model of the app owner for this technology.
4. Adoption of a specific license in the market sector.
5. Existence of a community.
6. Existence of patents on the technology underlying the code. In this case, a license contemplating a patent grant would be preferred.
7. Existence of a registered trademark that the rights holder wants to prevent from being used in connection with derived software.

For this chapter, the most relevant is the question of ensuring compliance with open source licensing on components included in your technology.

Figure 9.2 Steps for releasing your app or technology, considering open source



Source: the authors.

9.7. Licensing out as open source

There is a growing community of open source apps and underlying technologies running mainly on the Android operating system but also on others. This section gives the steps and

best practices for releasing mobile app technologies as open source software (not just the app itself, but component parts, SDK and libraries), and for increasing the benefit of being in the open source community: how to manage contributions, organize the community and managing the release of software versions.

In fact, open source is suitable for non-differentiating software, such as general purpose databases, operating systems and infrastructure, where companies no longer gain a significant competitive edge by keeping the technology proprietary. Joint development projects under an open licensing regime also allow companies to lower development costs by sharing efforts with others without losing a competitive advantage.

9.7.1. Motivation

There are several motives for releasing a technology as open source. The first is that it is required by a license on technologies embedded in the app; if an app developer incorporates strong copyleft licensed components (such as under the GPL or AGPL license) in their technology, if they then want to license the technology to an app owner, or distribute the result as the app owner themselves, they will usually have to do so under the same license terms, which in practice may make the technology available to everyone. If this is going to happen, it may be better to release the technology publicly in an open source software management platform managed by the developer and take advantage of the benefits of an open source community.

However, many open source projects, particularly complex ones, have developed because of the activities of a community of individuals and organizations that provide development, testing, debugging and governance; that is, there are benefits derived from a shared approach to software development. For example, bugs may be fixed faster or more testing might be carried out for different use cases or technology platforms. Another technical benefit is that the code contributed to a project is maintained (if the project is active and sustainable) by the project itself, so the contributor does not necessarily have to do this by themselves (this is

called upstreaming). Further, due to the need to share knowledge and understanding of the software coding, it becomes more standard and stable, and may even avoid separate versions (forks) that are then abandoned or are more costly to maintain. So, many projects are released as open source to take advantage of these technical benefits.

Further, open source licensing is an efficient way of regulating IP in large, medium or even small-scale collaborative projects, the Android kernel being an example. The rules regarding licensing of the contributions are transparent and known (often, the project license or a contribution license agreement) and this levels the playing field among entities and individuals contributing to the project. It not only ensures transparency and peer review of contributions, which lends itself to more stable and secure software, but also enables individuals and small and medium businesses, from any part of the world, to participate in the project.

Example: OpenMRS

OpenMRS is an open source platform and app for managing electronic medical records, founded on the principles of openness and the exchange of ideas, software and strategies for deployment. It is crafted to function effectively in resource-constrained environments and can easily be customized by incorporating new data elements, forms and reports. The OpenMRS community has developed a range of downloadable add-on modules to enhance its capabilities. The app for Android is hosted here.

License

The OpenMRS code is distributed under the MPL 2.0 license with a healthcare disclaimer. The MPL 2.0 is a copyleft license and incorporates disclaimers and a limitation of liability. In addition, OpenMRS disclaims warranties on compliance with privacy laws, or regulations or clinical care industry standards and protocols, and it makes explicit that contributors to the code are not liable for any indirect, special, incidental or consequential damages of any character.

Compliance

OpenMRS core's GitHub page includes a NOTICE.md file that includes the notices, license texts and disclaimers of all open source dependencies, and a persistent link to their repositories, where their original source code can be found.

Developers and organizations involved in app technologies do not have to be the project founders and maintainers. They can participate in an open source community at any level, from reporting an issue and contributing a fix, to being actively involved in project maintenance and governance. There is no obligation, but being involved does usually bring benefits in terms of acquiring knowledge and influencing the project roadmap.

For all that, releasing software as open source means that the rights holder is licensing, to all third parties, the core technology and knowledge embedded in the code, so that they may use this to build alternative (and even competing) products. This may be mitigated or managed by determining how much of the app technology is released as open source, what part of the app, and under which license.

Example: image recognition.

A technology developer creates an image recognition technology that can be used in a variety of applications (fashion, industrial machinery, components, among others). The system enables mobile users to point the device camera at an object or other image and identify it (an article of clothing by a specific designer, or spare part from a manufacturer, for example), and then link to online information or processes such as catalogues or instructions, or a sales process. To facilitate uptake of the technology, the developer distributes under a permissive open source license (the MIT license), an open source software development kit (SDK) for embedding in apps built by third-party clients, to install in the user's device. Such permissive licensing promotes interoperability and easy integration with apps and third-party technologies built by third-party clients and other technology partners.

Weighing up the pros and cons of open source discussed above is a way to make an objective, considered technical, legal and business decision on releasing app-related technology as open source.

9.7.2. Process

Releasing app-related software under an open source license does not mean just publishing the software on an open repository and putting a license on the code. This would be sufficient but does not mean all members of the ecosystem in which the app developer or publisher is involved will automatically take up the technology, make new contributions or be active in the project.

First, there are legal requirements. If the developer is including third-party (open source) components, then the compliance requirements must be adhered to. The project must respect the licensing requirements of these components, including all copyright notices and license texts, and ensure compatibility between inbound licensing on components and the project outbound license. Further, release of creative work needs a license, given the default rule under copyright is 'all rights reserved'. The project must choose a license and visibly include this in the repository where the code is published (best practice suggests that mention must be made in each file of the source code).

There are also recommendations as to technical aspects, such as building the software in a modular and standardized manner and publishing appropriate technical documentation to help build a community and share the technology with third parties.

Finally, if the aim is to obtain contributions from third parties, and collaboration on software development, then most open source projects also publish rules of governance, including on licensing of inbound contributions, and technical decisions made for future project development (the roadmap), and on how decisions are taken in the community.

Open Source Community Guidelines

GitHub, one of the largest open source software repositories, has published community guidelines for new projects. More information is available on the GitHub website, www.docs.github.com/en/issues/planning-and-tracking-with-projects/creating-

projects/creating-a-project and www.docs.github.com/en/communities/setting-up-your-project-for-healthy-contributions.

Other guidelines have been published on the Github website by the TODO group, www.github.com/todogroup/todogroup.org/tree/main/content/en/guides, and on the Open Source website, www.opensource.guide/starting-a-project/.

Following such recommendations (and other guidelines) helps project sustainability. Open source projects can become what is called abandonware, because the founders are no longer interested in supporting and improving the software, or because maintaining the project requires such individual effort on behalf of the founders that they no longer have the resources for it. Sustaining open source projects is difficult, requiring certain financial stability, an active and dynamic community and community management, and continued technological relevance.

One model for sustainability is to dedicate revenue from licensing the software IP in a more traditional manner (as a business offering) to cross-subsidize community activities and progress of the open source version of the technology. There are several such business models relating to open source software in the mobile app ecosystem, including:

- Dual licensing: providing the software as open source for the community but also licensing it under a traditional proprietary license for revenue to those entities that do not want to license it under an open source license.
- Service provision: providing revenue-earning professional services around open technologies for a fee, such as technical support and maintenance, integration services and security fixes.

It is important to note, however, that open source licensing is a software development and licensing model and not a business model as such. Thinking about open source software-based business models rather than open source business models may provide better insight

into how to create mobile app products and technology offerings, adequately license the IP in the project, and achieve sustainability.

9.8. Specific open source issues and mobile apps: architecture (apps, backend/servers, SaaS/webapps) and app stores

As noted in the introduction, open source software is frequently used in mobile app technologies, and in the ecosystem, all the more so because Android (one of the main operating systems for mobile devices) is licensed as open source. This section presents cases where open source is used in the mobile app technological environment, and the IP management and licensing issues to consider (in the app itself, on the server, integrating with other technologies, and providing web apps or software as a service). It looks at how app stores and app store contracts may impact the obligation to make source code available, and the responsibilities for compliance within this framework.

9.8.1. Use cases of open source in mobile app technologies

Open source software can arise in many parts of the mobile app technology environment, with differing implications for IP management. Common use cases include:

- **On the device (app):** the device app itself may include open source components, including specific features such as embedded keyboards, connectivity, user authentication and other functionality. Regarding IP and licensing, software running on the device will have been distributed (via the app store or directly). The terms of all open source licenses applicable to each component contained within the app will need to be compliant in terms of attribution, license texts and access to source code. Further, the app itself will need to be licensed out to users under an end-user license agreement, with appropriate terms as to copyright and other IP rights (including patents on any invention embedded in the app, or trademarks on the interface).

- **On the backend (server):** many mobile apps, particularly professional apps for enterprise or scientific purposes, include both the app itself on the device and a backend on a cloud server to which the device connects. This backend is usually a sophisticated software stack with many data processing methods and functionality, data and security management, and connectivity with other apps or services. So, the backend will often include mature open source components such as database engines, content servers and authentication functions. Regarding open source IP management, this software on the server is not being distributed, and because the conditions contained in almost all open source licenses only have implications when the software is distributed, the compliance obligations for services running on your server are relatively light.
- **Software as a service (SaaS):** some apps are merely an interface to functionality on the server. However, even if the app's main functionality is provided remotely on a SaaS basis, with the code running on a server, the solution may be providing some functionality using browser-based code, such as JavaScript or Single Page Application technologies, which is distributed to the user. Licensing requirements on this distributed code must be complied with.

An open source operating system for apps: Android

The Android open source project manages the Android mobile operating system and is run by the Open Handset Alliance led by Google Inc. Android is a modified version of the Linux kernel, with other software included specifically for managing mobile devices. Often the device manufacturer versions include extra proprietary software (non-open source), such as the versions released by Google every six to 12 months, and device drivers and other embedded binary software. Google retains its Google Play Store and Google Mobile Services as proprietary code, which are not always used in emerging markets as they tend to employ only the open code and not the Android trademark.

In terms of IP management, Android is mainly licensed under the permissive Apache Software License 2.0 but also includes other licensed components such as the kernel under the GPL 2.0. Its source code can be found here, and licensing information here. Contributions to the project are made under Google's Android Contributor License Agreements, individual and corporate. The Android trademark is not openly licensed but a registered trademark of Google, which it leverages to enforce compatibility of versions with the Google Android release; only compatible versions may carry the Android mark. Interestingly, the green robot logo often associated with Android is freely licensed under the Creative Commons BY 3.0 license.

Mobile vendors such as Samsung or HTC can use the Android operative system freely and include their own user interfaces and software applications. App developers can develop any kind of app for Android and test them freely, either on a device or on an Android simulation. One advantage of this open source operating system is that app developers and publishers have access to/right to use core features of the operating system under the license terms, and can adapt, reduce or extend the system for specific use cases, while the Android open source community provides updates, security fixes and new features that can be included in community releases or taken up by device manufacturers and the next version of Android itself.

9.8.2. Open source and the software development process

As we have seen, often the app owner is not necessarily the (only) developer of the app technology and will frequently subcontract to a third-party agency or developer. The owner is not so much in control of open source usage, and it is important they have visibility and are able to impose and verify compliance obligations on the developer.

The following checklist will help manage open source in the context of this relationship.

Checklist: owners and open source in their apps

1. Verify if you or a third-party developer have included open source components in the app.
2. Obtain, internally or from the external developers, the full list of open source components (SBOM).

3. In the software development contract, obligate the app developer to follow the above checklist for compliance and provide you with a copy of the SBOM, all copyright notices and other steps and information to comply with open source licensed components and libraries.
4. In the software development contract, ensure the app developer is responsible (as developer) for complying with open source license obligations in distributing the code to you (as owner) and liable for any breach.
5. In the software development contract, if releasing your app as a proprietary code, consider if you wish to prohibit the use of strong copyleft licensed components.
6. Ensure you have a copy of all the source code that corresponds exactly to the app binary, and if necessary, scan the source code for license information to verify the compliance artefacts.
7. Include the list of open source components in any distribution of the app (for example, in an app store), together with all compliance information (for example, in a licensing option in the menu).

9.8.3. App stores

Distributing software and content in the app stores is considered a distribution or communication to the public under copyright laws, which means the app owner must have these rights in the app technology to be able to publish the mobile app. Further, the app store terms require the app owner, as publisher, to authorize the store to redistribute or communicate the app to the public. So, it is essential the app owner ensures it has these rights to distribute or communicate in all technology that has been developed, either internally or with a third-party app developer.

In addition, in open source license terms, publishing the app in the store is a distribution under the license, and therefore the owner must comply with the open source license conditions on distribution (discussed above in terms of compliance). For iOS and Android-based mobile apps, compliance is reasonably straightforward when the app contains only permissively licensed code. However, once code under various copyleft licenses is incorporated, it

becomes more complex, given the owner (and potentially the app store, as secondary publisher of the code) may have to provide access to source code and installation scripts of this copyleft code (such as under GPL or LGPL licenses). For the iOS Apple App Store, compliance analysis may be more complex as the terms are more complicated.

The Apple Developer Program License Agreement terms on open source

"3.3.22 *If Your Application or Your Corresponding Product includes any FOSS, You agree to comply with all applicable FOSS licensing terms. You also agree not to use any FOSS in the development of Your Application or Your Corresponding Product in such a way that would cause the non-FOSS portions of the Apple Software to be subject to any FOSS licensing terms or obligations*." [(a)]

This means:

If any open source software is included in your app and you want to distribute it through Apple's App Store, you have a contractual obligation to comply with the licenses of the open source components used.

You also have to ensure that any copyleft open source components used does not affect Apple SDKs, iOS, watchOS, tvOS, iPadOS, visionOS, and/or macOS, the provisioning profiles, FPS SDK, FPS Deployment Package, and any other software that Apple makes available to developers.

[a] Apple Developer. "Apple Developer Program License Agreement." developer.apple.com. Apple Inc, Dec. 22, 2023. < https://developer.apple.com/support/terms/apple-developer-program-license-agreement/ >

Google's Play Store provisions on open source

- Google Play services guide on open source states that developers are responsible for displaying notices for the open source libraries used in their apps.
- Google makes available a set of tools designed to provide developers with a simple way to express the open source software notices of libraries used in their apps, as well as open source libraries used to create the Google Play services libraries compiled into the app.

- One such tool is a Gradle plug-in that collects license terms from included libraries, as declared in their “POM” files, and creates an activity that can be used to display these terms.

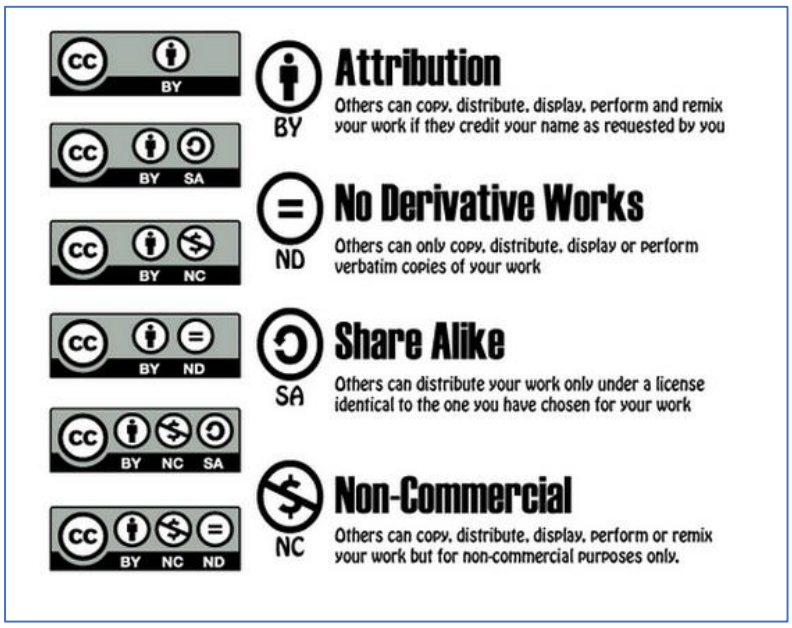
9.9. Other types of open licensing

Software is not the only IP asset commonly licensed openly, under the principles of open access, use and modification. While Open Science, which provides open access to scientific knowledge, is spreading around the world, particularly in university and government research and development projects, other mature and expanding open communities are relevant in the app sector.

9.9.1. Open content licenses

The largest “open” movement that is not software is open content licensing, which started in the 1990s with the GNU Fee Document License but is now mainly supported by the Creative Commons suite of content licenses. Such licenses are mainly drafted for text, audio, audiovisual and visual, and other artistic works, and offer a variety of options, from the fully open CC-0 (basically a dedication of a work to the public domain), to the CC-BY-ND-NC, the most closed license (attribution, no derivative works and no commercial use).

Figure 9.3 Series of Creative Commons licenses



Source: Creative Commons. "About CC licenses." *creativecommons.org.* 2019. <*www.creativecommons.org/share-your-work/cclicenses/*>.

Using the ND (no derivatives) and/or NC (no commercial use) attributes means the license is not open but still permits open access, reproduction and publication (for non-commercial use, with NC attribute). Many apps use and integrate graphic and textual content, and for this purpose developers and owners may find a vast amount of available materials under Creative Commons licenses, as well as publishing their own works in a digital manner on the app, under an open content license.

Works under CC licenses

Creative Commons (CC) indicates that there are more than 2.5 billion works available under CC licenses. Many of these can be searched here.

9.9.2. Open data

Digital technologies are built on, use and create data, which is becoming increasingly important, all the more so with data used for training machine learning or AI systems. Think geographic data for geopositioning and maps, health data in your health and fitness app, or

economic or financial data in your banking app. While the data sector is behind software in terms of experience, there are standard open data licenses such as the Open Data Commons Open Database License (ODbL)[44] that can be used to share data on an open basis. Also, many data projects use Creative Commons licenses, particularly CC-0 and CC-BY for science projects, to maximize data sharing. Just like open source licenses, if a project is using third-party data, it will be important to review and understand the data license and ensure compliance with downstream terms regarding use, reuse and (re)publication.

OpenStreetMap

OpenStreetMap is a project that publishes open geographic data, creating a map of the world that can be used in apps for geopositioning and similar functions, which are common in apps (tracking deliveries, distance checking, route building, among other things). OpenStreetMap data is licensed under the Open Data Commons Open Database License.

Barcelona Open Data

Open Data BCN is a public open data platform offering up to nearly 600 sets of data on Barcelona, which can be freely downloaded and used by app developers. Most datasets are published under the CC-BY 4.0 license. This is one of the many public open data repositories, which reach from Buenos Aires, Argentina, to Cape Town in South Africa, and from Kerala, India, to Portland in the United States of America.

As explored in chapter 4, in IP terms there are no harmonized rules regarding datasets such as there are for copyrights and certain other IP rights under international treaties. So, understanding local laws and rules on data access and use is important.

[44] Open Data Commons. "Open Data Commons Open Database License (ODbL) v1.0." *opendatacommons*.org. Open Knowledge Foundation. <www.opendatacommons.org/licenses/odbl/1.0/>.

9.10. Legal issues in open source licensing: a quick guide

Not all is pacific in open source IP licensing. As with traditional software licensing, rights holders may and do claim that software, including apps, infringes their rights. Compliance with licenses is just as important with open source software. With open source, claims might arise, for instance, if open source components are used or distributed in the app in breach of their license terms, including not providing copyright notices or complying with a copyleft requirement that the source code be made available. Further, there may be patented inventions being exploited in the app (or the backend), through manufacture, distribution and use of patented technologies by end users that may lead to patent-based claims against the software developer and publisher, and the end user.

In practical terms, this can be costly and time consuming, and dire from a business perspective if a court issues an injunction preventing an app's publication, distribution or sale until the matter is resolved. Handling such enforcement claims requires specialized technical and legal advice, and the global reach of app technologies makes enforcement and defence complicated and expensive (see chapters on IP protection and on dispute resolution).

However, one difference with traditional software licensing, generally speaking, is that rights holders seeking to enforce their rights under an open source license aim to make the alleged infringer comply rather than pay an indemnity. Holders of copyrights in the openly licensed technologies are less likely to be interested in claiming significant damages, though they might seek legal costs.

Running an open source project and receiving contributions from third parties also requires clear handling and management of IP and licensing. If contributions are not correctly 'licensed in', those responsible for maintaining the project, and anyone downloading and reusing the open source software, may be open to claims (mainly based on copyrights) that the project code is not compliant. This also makes downstream compliance by app developers and publishers a difficult if not impossible exercise.

9.11. Conclusions

There are key actions that app developers and publishers must take in relation to open source software.

First and foremost, they must comply with open source licenses when distributing the app technology with regard to license compatibility, copyright attribution, licensing information and access to source code.

Second, as discussed in chapter 5, many organizations seeking to develop an app will employ an external developer. They will almost always make use of open source software. The owner must ensure the developer has a procedure for disclosing the use of open source code and for providing, on delivery, a complete list of all components used. This will enable the owner to comply with the license terms. The development contract may also prohibit the use of certain types of open source licenses whose terms may conflict with the owner's own licensing model.

Third, app owners should review and comply with app store requirements. When developing an app to be distributed through an app store, the owner should be aware that app store agreements have provisions that may restrict the extent to which open source components can be used. It is important to ensure that the components used in a developer's app do not contain code licensed under terms that could cause problems under the app store agreement, or be incompatible with the license the developer is using under its customer agreement. This can be included in the app development contract and managed from the start.

And finally, the app owner needs to incorporate appropriate terms in the app end-user license agreement (EULA) that the end user is required to enter into before using the software. Typically, when you run an app for the first time as a user, you will be presented with a box where you must register, and that might require you to agree to a license agreement. When releasing the app, it is important the owner ensures it does not breach requirements specified

in any of the open source licenses of the components used, in particular copyleft components requiring use of the same license terms and providing access to source code.

Key takeaways

- There are many open source technologies used in mobile apps.
- Open source licensing is a license model that enables users to use, reproduce, transform and (re)distribute software works.
- There are a variety of open source licenses, from permissive to copyleft.
- All licenses require you to retain and publish with your app appropriate attribution and a copy of the license text.
- Copyleft obligations require you to use the same license and provide access to the source of the work and derivatives thereof, in the event of redistribution.
- If you do use these open source works, ensure you comply with the license obligations, in particular copyleft obligations.
- If you contract out the app development, ensure the developer is aware of these same obligations and supports compliance.
- You may also wish to open source your own technology or app, in which case you need to do the same compliance check and also decide on what license you want to use for publication.
- There are also open licenses for artistic and literary content (for example, Creative Commons) and data (for example, Creative Commons or Open Database licenses), and these may be relevant for your app if you embed or use these types of works.

9.12. Useful links and resources

WIPO, *Open Source for Mobile Apps*.

Open Source Initiative, The Open Source Definition.

Jolts, *The Journal of Open Law, Technology and Society*.

Chapter 10. Ensuring respect for IP rights in mobile apps

10.1. Introduction

In the world of mobile applications, IP rights play a fundamental role, and such rights must be respected. On the one hand, it is important to make sure our mobile apps and actions do not infringe IP rights owned by others, but on the other hand, to protect the value of our rights, it is fundamental to actively ensure that other entities are not using them without consent.

This chapter focuses on the measures to implement, and when in the app life cycle to implement them, to avoid infringement of third-party IP rights. The second section considers the measures to protect IP from unauthorized use.

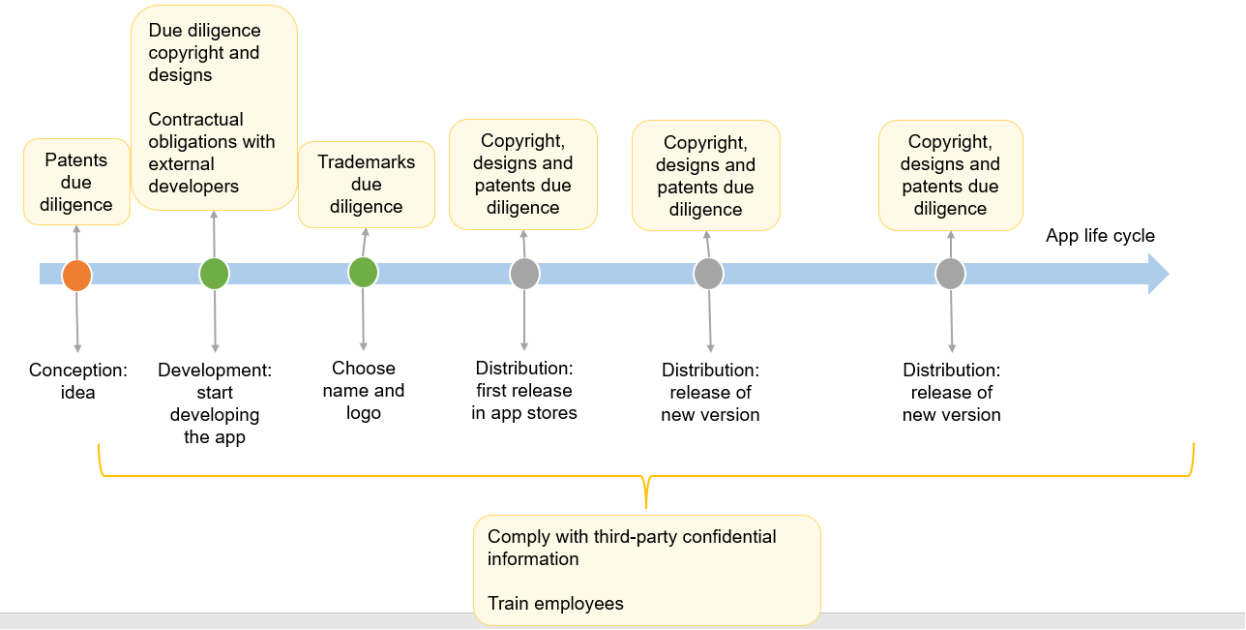
The concept of "Rightsholder"

Given different key parties – the app owner, developer, or even third-party licensee, for example – may retain rights and be responsible for securing and enforcing them, in this chapter we will refer to them all indiscriminately as the rights holders.

10.2. Ensuring your mobile app does not infringe rights owned by others

When creating and commercializing a mobile app, taking appropriate actions to avoid infringing someone else's rights is imperative. All infringements, irrespective of whether accidental or intentional, are prosecutable and can lead to negative consequences. For this reason, it is advisable to follow the recommendations outlined below to reduce the risk of third-party rights violation.

Figure 10.1 Actions to reduce third-party rights violation during app life cycle



Source: the authors.

10.2.1. Performing due diligence in relation to preexisting IP rights

The first recommended action is to perform due diligence throughout design, creation and commercialization of the app. This entails researching and analyzing existing IP rights before taking decisions that may affect or involve IP rights.[45]

In particular, we recommend performing due diligence with respect to the following.

a) Trademarks

As discussed in chapter 4, trademarks are extremely relevant in the mobile app market. End users recognize one app in the plethora of mobile apps available in app stores thanks to the app's name, logo or colors – these are the first elements they see, even before, say, functionality. For this reason, when considering a name or logo for the app, or other elements

[45] See World Intellectual Property Organization. The Role of Intellectual Property Rights in the Development and Commercialization of Mobile Applications. WIPO, 2021: sect. 2.1.

that can be protected by trademark law, and before even thinking about applying for legal protection, conducting research on existing trademarks is recommended.

In particular, the app owner or publisher should consider the following for the territory where they want to commercialize the app:

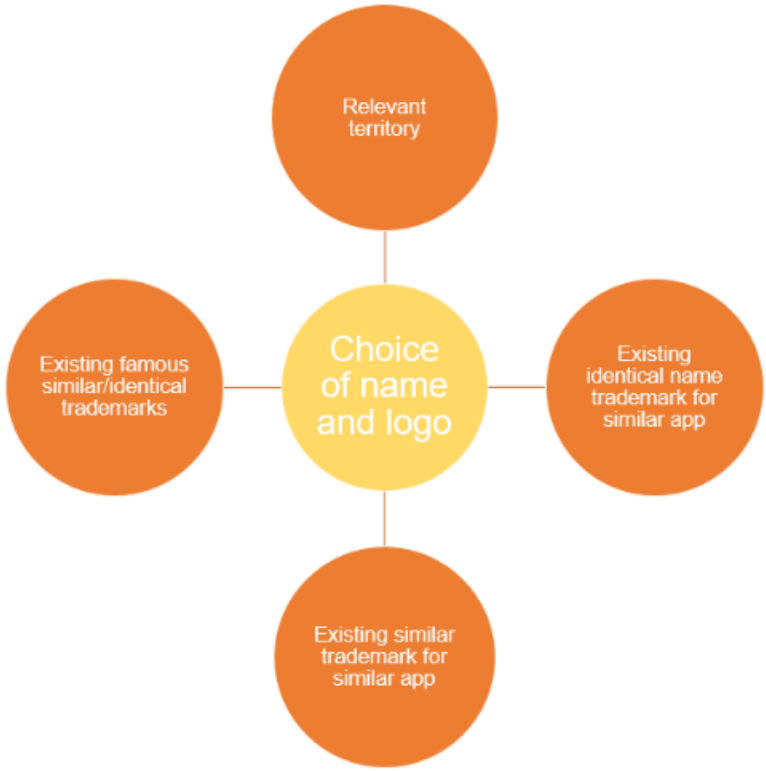
- Check if a similar app exists with an identical name or logo. In such a case, applying those marks should be avoided, as it would likely be a trademark infringement.
- Check if a similar app exists with a similar name or logo. End users could be confused as to the origin of the app, and it could be a trademark infringement. In this scenario, we recommend avoiding the use of names or logo initially considered.
- Check if the name or logo are similar or identical to famous ones whose rights are owned by other people. Such trademarks have additional protection and using them in the app could lead to a trademark infringement.

A ‘similar app’ means a mobile app in the same sector. If the app is a social network, consider other social network apps, and if it is an e-commerce app, look at the e-commerce sector and related sectors or services for the same or related products.

Further, we strongly recommend extending research to other territories not initially contemplated, for several reasons, including: (1) app stores make mobile apps potentially available worldwide, and (2) owners and app investors often want to scale up and expand their territories of operation, and it is desirable to do so under the same name or logo.

The elements to consider in researching existing trademarks are provided in figure 10.2.

Figure 10.2 Elements to consider when choosing app name and logo



Source: the authors.

Research into preexisting trademarks can be complicated, and legal advice from an IP lawyer or IP professional is recommended.

Checklist: due diligence on existing trademarks

- Identify the territories you plan to target:
  - consider that app stores potentially make the app available worldwide.
- Identify the similar mobile apps in the market and targeted territory:
  - check the logo and name they use.
- Avoid copying or using an identical or similar name or logo for the app.
- Avoid copying or using names or logos similar or identical to famous trademarks, even if they are registered for different products/services:
  - avoid names like Nike, Louis Vuitton and Ferrari, for example.

Tip: look for an IP lawyer or IP professional to check on existing trademarks. There are also online tools that can help, such as the EUIPO TMview service.

b) Copyrights

Copyrights and the code

Nowadays, it is unlikely mobile apps, or software in general, are developed without using a piece of code (or other content) that already exists. The use of open source software and open content under Creative Commons licenses is widespread, and, while code reuse is one of the purposes for which open source was created, it is important to stay within the limits of a license and comply with its obligations (see chapter 8 for details on open source licenses and how to comply with them).

The same happens when using non-open source code licensed by other entities, such as app SKD developers, or an app developer's own existing software embedded in an app by the developer. Such licenses usually include restrictions and prohibitions, including reporting and royalty payments, and compliance is mandatory.

Last but not least, when using code or content from the Internet, permission to use the material must be checked. This permission can take the form of a reference to a license, or to a clause included in the terms and conditions of the website where the material is published (see box below for examples). And note that there is much software on the Internet (snippets of code, examples, suggestions from developers) that has no license, so beware.

Examples: permissions (or prohibitions) to use code published online

1 You may find an open source license included in the license section of a repository, such as the following MIT license:

© 2023 John Developer

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

The software is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the Software or the use or other dealings in the Software.

2 Or you can find sentences such as the following in website terms and conditions:

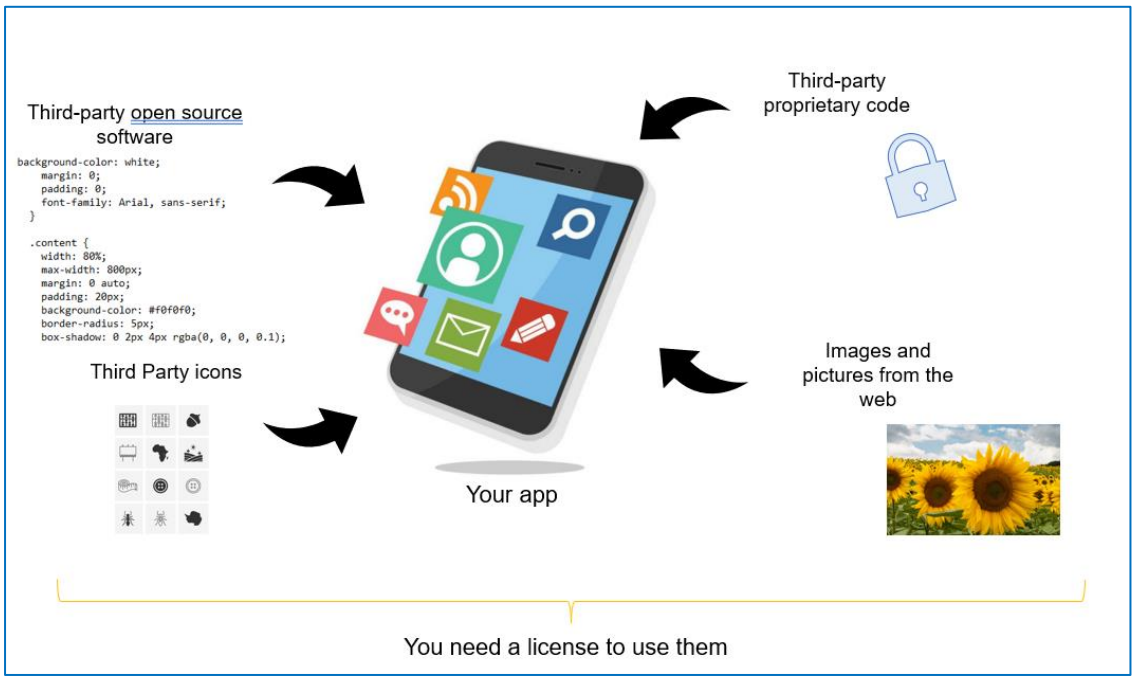
- Prohibition to use the content for commercial/business purposes: "*The content of this website, including any image, text and software code, can be used for personal purposes only. All commercial or business purpose is strictly prohibited*."

- Allowance to use the content for commercial purposes as well: "*The content of this website, including any image, text and software code, can be used for any purposes, including commercial ones. You can copy, reproduce, distribute and make available to the public the content of this website, provided you mention the website owner as a source of the content*."

Copyright and interface elements

Copyright protects artistic works, including drawings, pictures and certain types of photographs, provided they are original (see chapter 4). When creating the interface of a mobile app, it is important to ensure no elements whose rights are owned by other entities are included in the interface or other parts of the app without the owner's consent. This means a picture found on the Internet may not be used if the rights owner has not provided their consent by including a license, such as an open content license or a tailor-made license. Using the content without appropriate consent would be a copyright infringement.

Figure 10.3 Elements that require copyright license to be included in mobile app



Source: webportal.com

Checklist: copyright due diligence

- Ensure a license exists when using software code from third parties:
  - if open source code is used, ensure compliance with the license on distribution; and
  - if proprietary code is used, utilize it within the limits and restrictions set out by the license.
- Ensure a license or permission exists to use elements created by other entities (drawings, pictures, icons, among others):
  - the license can be explicit (Creative Commons license), or it can be included in the terms and conditions of the website where published.

c) Design rights

Design rights are especially relevant for app interfaces, as outlined in chapter 4. While designing the app and its user interface, and making any update or new version that implies changes in the graphical user interface (GUI), it is important to ensure that no existing design rights are violated.

Attention must be given to the existence of designs protecting not only GUIs or GUI elements, but also shapes and decorations of physical items that may have been digitalized and included in the app; for example, icons. In general, avoiding the use of any protected design is recommended.

Checklist: design rights due diligence

- Ensure no element included in the user interface is a registered design owned by a third party:
  - look for existing GUI/GUI elements registered as designs; and
  - also look for existing registered designs of a physical object you may have included in your GUI.
- When planning to use elements registered as designs owned by other entities, contact the owners and request a license.

d) Patents

As explained in chapter 4, patents may protect elements of mobile apps and their functionalities, GUIs or technologies underlying the app, both in the mobile device or in the architecture and coding of the backend server to which it connects. Such elements are less visible than, for instance, the interface design or images included in the mobile app but must be considered.

Due diligence with respect to patents consists of checking that no patent, or patent application exists, on any functional elements of the user interface or technology underlying the mobile app in the relevant territory of commercialization of the app – generally speaking, worldwide. This is called a freedom to operate search (FTO) and it can be carried out by local or international patent agents. If a patent does exist, contact the patent owner and request a license.

As for trademarks, it is wise to extend the research to territories that are not initially targeted, given: (1) app stores potentially make apps available globally, and (2) scaling up and

expanding territories of operation is usually desirable for app owners and their investors, so FTO is required in these potential new territories.

Checklist: patents due diligence

1. Identify the territories that you want to target:
   - consider that app stores potentially make your app available worldwide; and
   - seek advice from a patent attorney (or IP agent).
2. The patent specialist will perform an FTO analysis to ensure no patent or patent application exists on any functional elements of the app, its UI or the technology underlying the app.
3. If a patent or patent application exists that covers your technology and processes in a relevant territory, contact the rights owners and request a license, or consider changing the products/processes so they do not infringe.

10.2.2. Requiring software and UI developers use only licensed third-party materials

While creating a mobile app, it is not uncommon to pay external developers and agencies to develop part of the code, content of the app, or part of the GUI, or to help out the internal software and content development team.

In that case, the owner has less visibility on the third-party code or material included in the app that the external developers deliver. As referenced in chapter 5 on development agreements, sourcing the technology from a third party, and lack of visibility with regard to the content of the mobile solution, does not exempt the app owner from responsibility if third-party rights are infringed. For this reason, there are specific clauses that we recommend including in contracts with external developers and agencies.

Table 10.1 – clauses with app developers

Content of the clause	Example of wording (simplified)
An obligation to use only third-party works if a license exists, and strictly comply with the license's restrictions and obligations. By including such a clause: • you ensure the developer is aware of this requirement; but • if this obligation is not complied with, the contract is breached and you can: (1) terminate it, (2) claim damages from the developer, and/or (3) recover loss on claims from third parties (indemnity, see below).	"If the developer incorporates any third-party materials, it must ensure that: (1) a valid license permitting such usage exists, and (2) all obligations and restrictions outlined in such licenses are complied with."
An obligation to disclose all third-party code and content embedded in and/or used to generate your app, and to include the license under which each of those pieces of code is distributed. This serves two purposes: • gain visibility on what is included in the app and under what license; and • third-party license compliance, including open source compliance.	"In case the developer incorporates any third-party materials in the deliverables, it must provide an accompanying list of third-party materials. The list shall include, at a minimum, the following details: name and version of the material, and name and version and a copy of the license under which the material is distributed."
The warranty that all deliverables are the original of the developer, or are duly licensed to them, and that they do not infringe any third-party right. If this warranty is not abided by and the contract is breached, this gives you options: (1) to reject the deliverable until it is compliant, (2) to seek compensation from the developer, or (3) if this is a material and continuing breach, terminate the contract.	"The developer warrants that all deliverables are original and that they do not infringe any third-party rights, including, without limitation to, intellectual property rights."

A specific indemnification for all damages deriving from third-party claims regarding IP infringement. With this clause, the developer will be obliged to indemnify the app owner; that is, bear all the loss and costs deriving from the claim.	"The developer will indemnify, defend and hold the customer harmless from and against all losses, liability, damage, cost or expense (including reasonable attorney fees) arising from any claim, action or proceeding brought by a third party against the customer to the extent based on any infringement of third-party rights, including, without limitation to, intellectual property rights." Note: This wording is not exact but rather a suggestion. Parties to the app development agreement should seek local legal advice.

Source: the authors.

10.2.3. Ensure no third-party confidential information or trade secret is used

If the app results from a collaboration with third parties (individuals or companies), or even from conversations with advisers or mentors, a nondisclosure agreement (NDA) should be signed at the start of the relationship. This protects the confidentiality of the information and trade secrets that may be revealed by the parties while they collaborate, even in phases prior to the collaboration if correctly drafted (see chapter 5 for information on NDAs).

NDAs typically provide for the following:

- The confidential information can be used only for the reason for which it was shared; for example, if it is shared to understand how to collaborate on a specific business project, it cannot be used by the recipient to improve its own product.
- The confidential information must be treated as confidential and protected by adequate measures.
- When the party disclosing the information requires so, or when the NDA terminates, all confidential information will be destroyed or returned to the disclosing party.

When confidential information or trade secrets are shared after signing an NDA, the provisions of the agreement have to be complied with, as well as the laws protecting trade secrets.

In particular, access to confidential information is restricted to employees on a strictly need-to-know basis, and they must be aware of the confidential character, as well as the specific purpose for which the information can be shared. Further, it is recommended that a confidential or trade secret policy is in place that protects your own information, and describes the process and measures to protect the confidential information of other entities that you receive in the course of collaboration or service provision, among other things.

Internally, app owners and developers should implement effective processes to ensure an app development project does not include data or information from other projects or parties, including maintaining separate development teams and ensuring that client information is only accessed on a need-to-know basis, and documenting these procedures as evidence of good information management.

Vis-à-vis respecting third party information in an app software development agreement, the above clauses on third-party rights should not be limited to IP rights, but also to any third-party rights, including trade secrets. Often warranties are extended, such that the developer guarantees that “no third-party confidential information is used or included in the performance of the development”, or more generally that “the developer will comply with all contractual obligations, including to third parties, in the performance of the agreement”.

Checklist: complying with third-party confidential information and trade secrets

1. Identify the confidential information shared by a third party:
    - identify the information shared, which can be in different formats (electronic, paper, oral, for instance); and
        - identify the information that is confidential or a trade secret, considering the definition of confidential information indicated in the NDA.information tagged as ‘confidential’ or as ‘trade secret’ or similar

wording, and information that should be considered confidential due to its nature).

2. Ensure only employees and external consultants who require access to the confidential information for the specific purposes outlined in the NDA are granted access:
    - always verify whether you are permitted to share the confidential information with external advisors, and thoroughly read the text of the agreement before signing it.
3. Ensure these individuals are fully aware of the confidential nature of the information and the uses for which it can be employed.
4. Implement appropriate measures to safeguard the confidentiality of the information

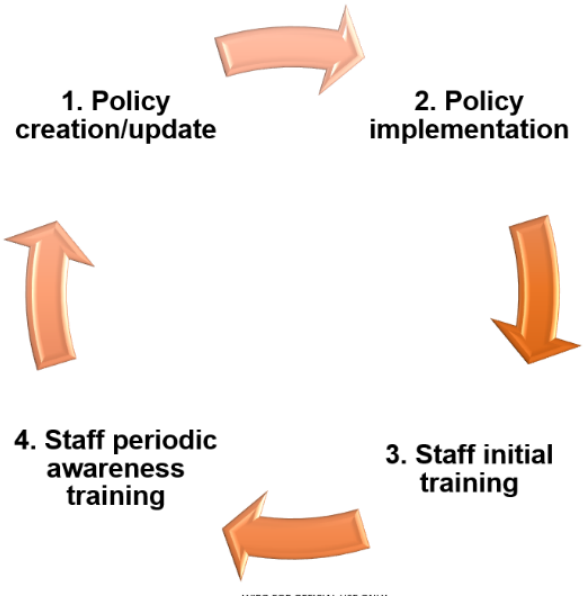
10.2.4. Train employees and other staff

When hiring coworkers or employees, the chance to supervise everything they do and all third-party material they use is limited. For this reason, and to ensure no third-party IP right is infringed or confidential information used without consent, it is vital to have policies in place that set out the prohibited conducts and the protocols to follow to avoid violations, and also to train the staff on such protocols.

The best way to avoid pitfalls is to perform periodical awareness training, creating a culture of IP awareness in the company. There is no need to become IP professionals, but knowing the basics and the actions to avoid, as well as when to ask for professional advice, is prudent.

The steps for effectively implementing IP policies within your company (and any type of policy) are outlined in figure 10.4.

Figure 10.4 IP policy implementation process



Source: the authors.

Checklist: training employees and establishing IP and information policies

1. Identify the key areas of IP that employees should be trained in, and establish policies (copyrights, trademarks, confidentiality) and relevant staff.
2. Seek help from IP professionals to create appropriate policies on the use of third-party materials and confidential information.
3. Implement and periodically update the policies.
4. Instruct staff and all new personnel and perform periodic awareness training.

Case study: Apple's alleged infringing of Personalized Media Communications patent in its FairPlay technology

The technology

Apple's FairPlay is a digital rights management technology used to decrypt/encrypt music, movies and apps. It was employed by Apple to ensure content purchased from the iTunes Store could only be accessed on authorized devices.

Claim

In 2015, Personalized Media Communications, LLC (PMC) filed a lawsuit against Apple for allegedly infringing a patent (Personalized Media Communications, LLC v. Apple, Inc.).

PMC claimed that Apple, particularly the FairPlay technology, infringed multiple patents owned by the company.

Outcome

In 2021, a Texas jury ruled that the FairPlay software violated one of PMC's patents, and Apple was directed to pay 308 million US dollars in damages. However, in January 2023, a US appeals court overturned the verdict against Apple, determining that PMC's patent was invalid.

Comment

Although this case concluded in Apple's favor, the eight-year duration undoubtedly incurred substantial legal expenses for both parties. This emphasizes the significance of conducting thorough preliminary searches (and periodic reassessments) to minimize the likelihood of facing a patent claim related to the technological foundation of an application.

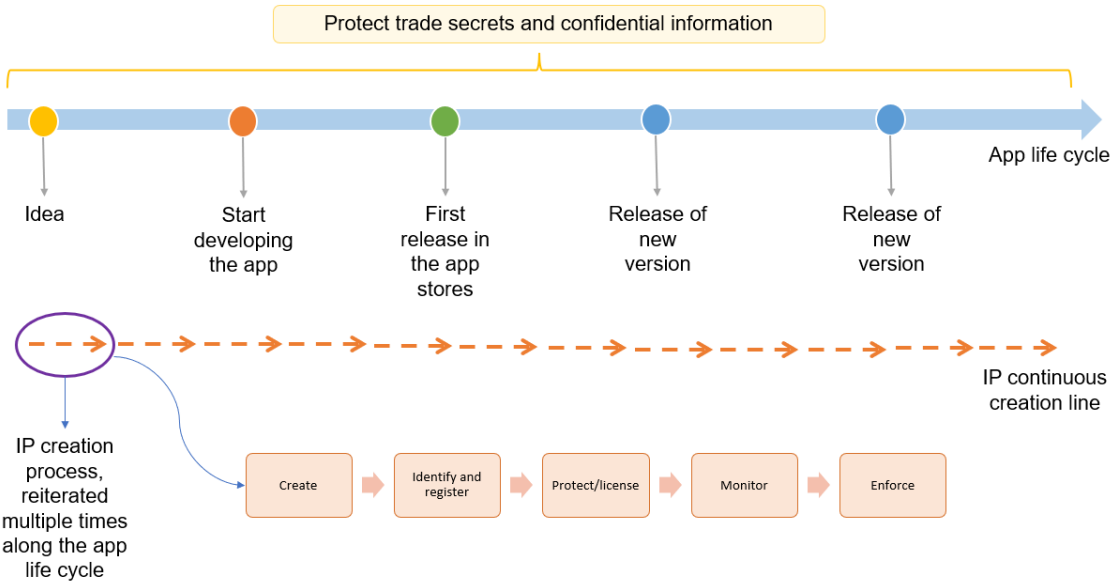
10.3. Protecting your own IP and enforcing rights

Now that we have seen how to ensure respect for third-parties' IP rights in the app life cycle and while operating a business, this section focuses on how to ensure respect for a rights holder's own IP rights. This will be discussed in a wide sense, considering not only the enforcement of those rights, but also how to make them effective.

Such steps include: (1) registering IP rights that can or must be registered, (2) including specific provisions on IP in the app's terms, (3) monitoring use of own IP by third parties, and (4) ensuring trade secrets are protected.

Steps (1) to (3) are not specifically related to the app's life cycle, but with the IP cycle in general. During the app's life cycle, IP is constantly generated, and for this reason the actions outlined must be reiterated multiple times. Then again, the protection of trade secrets is an ongoing work, from creation of the idea to the possible discontinuation of the app.

Figure 10.5 Protection of IP and trade secrets along the app life cycle



Source: the authors.

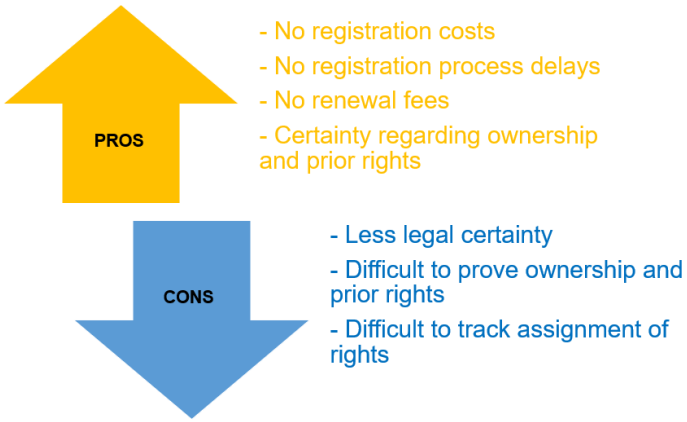
10.3.1. Identify assets and register IP rights that can be registered

The first basic step is to identify the relevant assets to understand what can be protected and how. We suggest referring to chapter 4 on the IP legal framework for details on IP rights, and chapter 7 on IP strategies to support financing and commercializing apps.

Certain rights such as patents, trademarks and designs come into existence only on their registration, while rights like copyright exist from the moment a work is created. For all IP rights that require registration to be valid and enforceable, it is vital to apply as soon as possible. We advise reaching out to an IP lawyer for guidance on the registration process.

Copyright stands apart, given it does not mandate registration: protection is automatic. This mechanism has its advantages and disadvantages.

Figure 10.6 Pros and cons of copyright protection



Source: the authors.

One disadvantage is the difficulty of proving ownership and preexisting rights. This can be partially solved by: (1) fixing the appropriate © notice on the work, and (2) registering or depositing the copyrighted work. Registration is not intended to establish rights over the work but serves as a means of proving the existence of rights, authorship and ownership, and generating a time stamp in case you need to assert your rights in court.

Steps and requirements for copyright registration are country-specific and often handled by government agencies.

Examples: government agencies handling copyrights registration

- India, Copyright Office, Government of India.
- United States of America, US Copyright Office.
- South Africa, Companies and Intellectual Property Commission.
- United Arab Emirates, Ministry of Economy, Copyright Department.
- Kenya, Kenya Copyright Board.
- Philippines, National Library of the Philippines.
- Spain, Registro General de la Propiedad Intelectual (Intellectual Property Registry).

The registration process depends on the office but there are common features among countries. The process starts with an application, where the copyright holder has to include details of the work such as the title and authors, a copy of the work, which will be kept confidential, and pay fees. The office reviews the application and supporting materials and, if approved, will issue a certificate of registration. Notarial deposit or registration in the blockchain is also a way of ensuring evidence of the work and prima facie copyrights in the work.

10.3.2. Include IP clauses in the relevant terms and conditions

When developing and launching a mobile app, end users will interact with the interface, its elements, logo and the app's name. Certain components of the GUI can be protected under various IP rights, including design rights, trademarks and copyright. To clarify the ownership of these rights or authorization to use them, we suggest incorporating a specific clause in the mobile app's terms and conditions or end-user license agreement (EULA). Moreover, within this clause, we recommend including a statement that outlines how the rights holder reserves their rights, indicating whether and to what extent others are permitted to use IP.

The IP clause should contain specific wording.

Table 10.2: contractual wording for IP in user contracts

Content of the clause	Example of wording
Identification of the rights on the material included in the app and their ownership. While all apps include certain material such as software code, not all include elements protected by, for instance, design rights. The content of this clause may vary, but we propose a standard text.	"All intellectual property rights on any content of this app, including, without limitation to, software code, images, video recordings, texts, icons and designs, are owned by or licensed to [name of the company]. The [app name] and logo are registered trademarks of [name of company]."
The reservation of rights and/or the permitted uses.	"All the above rights are reserved in favor of the company. Unless otherwise indicated, all acts of reproduction, distribution, modification, removal,

Specific wording depends on what you want to allow third parties to do with your content. We propose a standard text preventing all uses, with the exception of making copies for personal noncommercial purposes.	handling and any other use of the content of the app without the prior express written permission of [name of the company] is expressly prohibited. Notwithstanding the foregoing, the content above can be reproduced for personal noncommercial purposes only."
Optional: if your app includes content that you want to allow other entities to reuse, you can apply an open content license. We propose a text setting out that all images and icons can be reused by providing attribution to the right holder, in application of the Creative Common's attribution license.	"The images and icons included in the app can be used, reproduced, modified and redistributed in accordance with the terms of the CC-BY license published at www.creativecommons.org/licenses/by/4.0/legalcode.txt."

Source: the authors.

In relation to agencies that develop apps as external service providers, to be able to enforce them, it is important to ensure that the app owner has ownership or exclusive licensing of all relevant IP rights. For this, we refer the reader to chapter 5 on IP contracts. The agency should (or must) assign all rights in the developed code and content to the app owner (or license the rights in a manner such that the owner may exercise and enforce them in courts).

10.3.3. Periodically monitor that no third party is using your IP without a license

Once you have identified your rights and taken steps to safeguard them, it is essential to ensure no one is utilizing them without permission. Monitoring is a proactive process that can be carried out in several ways, depending on the type of IP rights. Common methods for monitoring IP include:

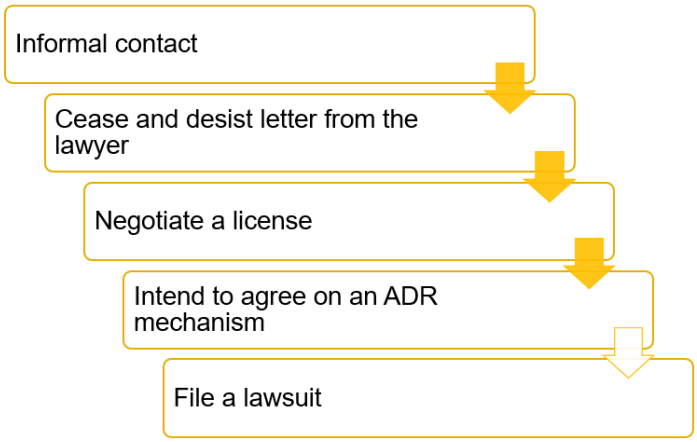
- Online searches: regularly perform searches using keywords related to your IP. While effective for identifying unapproved use of copyrighted work or trademarks (graphical elements that are more visible), this is less suitable for patent rights (over technical methods or processes).

- App store searches: periodically check mobile app stores to identify any apps that may be infringing rights; for example:
    - if the app name and/or logo is registered as a trademark, check whether there are apps with similar or identical names or logos; and
    - if parts of the GUI are registered as design, check whether there are apps using the same GUI elements.
- Competitor monitoring: regularly monitor competitors apps to determine if they have copied any protected features.
- Search engine alerts: specifically for trademarks. Alerts should be set up and notifications through search engines based on specific keywords.
- IP office notices: certain IP offices send notifications regarding attempts to register rights similar to yours; for example, the European Union IP office (EUIPO) will inform the right holder if someone has applied for a trademark that is similar or identical. This allows you to decide whether to oppose the registration.
- Marking your IP assets: with specific regard to copyrighted works such as pictures, videos and phonograms, they can be watermarked to identify unauthorized copies more easily.
- Monitoring services: there are companies offering IP monitoring services, allowing IP proprietors to identify infringement and take action. Such services are offered for a fee and enable you to detect infringement of various IP rights.

10.3.4. Legally enforce your rights

When someone is using IP without consent, steps should be taken to stop the infringement. There are different actions available, which are usually taken progressively.

Figure 10.7 Legal actions to enforce IP rights



Source: the authors.

The steps of this process include the following:

1. **Informal contact**: for a friendly approach, the first step involves reaching out to the infringer and informing them they do not have a license to use your IP, and that the use infringes your IP rights. This approach is often effective if they did not intentionally infringe and are willing to remove your content or stop using your IP; for example, if someone uses GUI elements you have registered as a design, or music and other copyrighted content.
2. **Cease and desist letter**: if informal contact has no positive outcome, or you prefer not to have initial informal contact, the next action is to have an IP lawyer send a cease and desist letter to the infringing party. This is a formal letter (usually prepared and sent by the lawyer), requesting they halt the infringing activities and refrain from them in the future. In certain jurisdictions, this is mandatory before filing a lawsuit.
3. **Negotiate a license**: if the infringer acknowledges your ownership of the IP and wishes to use it, an option is to negotiate a license. This enables them to use your IP lawfully, with your consent, against payment of royalties or other license obligations.

4. **Attempt ADR**: when the parties are open to submitting the management and eventual resolution of the dispute to an ADR process, this may offer a less onerous mechanism in a single forum, with a confidential and enforceable result (settlement).
5. **File a lawsuit**: should the infringing party persist in their actions after receiving the cease and desist letter, you might consider initiating legal proceedings. The specifics, including costs and duration, vary by country, and it is advisable to consult a local lawyer for guidance.

For more details on ADR and judicial dispute resolution, see chapter 6.

In addition to directly addressing the infringer, if the infringement is through another app, then the IP owner may request app stores take down or at least suspend the allegedly infringing app. Most stores have a specific procedure and online channel for this and usually respond quickly (otherwise, depending on jurisdiction, they may be liable for contributory infringement). This is often an effective and dissuasive measure but the claimant must be sure of the breach, given it could backfire if the alleged infringer is not infringing and brings a counterclaim for commercial damages.

Recommendation

An owner of a game app based in Brazil identifies another game app located in the United States of America that has recently been published in an app store with a confusingly similar brand name.

What should the app owner do?

- Check whether its brand name is protected by a trademark and the scope of this protection. If not, there are scenarios where protection can be conferred through unregistered trademark protections and even competition laws. Always seek expert advice.
- Investigate where the similar name is being used anywhere besides the app store. This may be important, for example, as to domain names (see WIPO's UDRP procedure, chapter 6).

- Secure proof. Try to get evidence to support your claim. Again, always seek expert advice.
- Make informal contact with the infringer.
- Send a cease and desist letter.
- Eventually send the app store a take down notice.
- Attempt to negotiate a trademark license with strict conditions.
- Attempt an ADR.
- File a lawsuit.

10.4. Confidential information and trade secrets: how to protect them and enforce rights

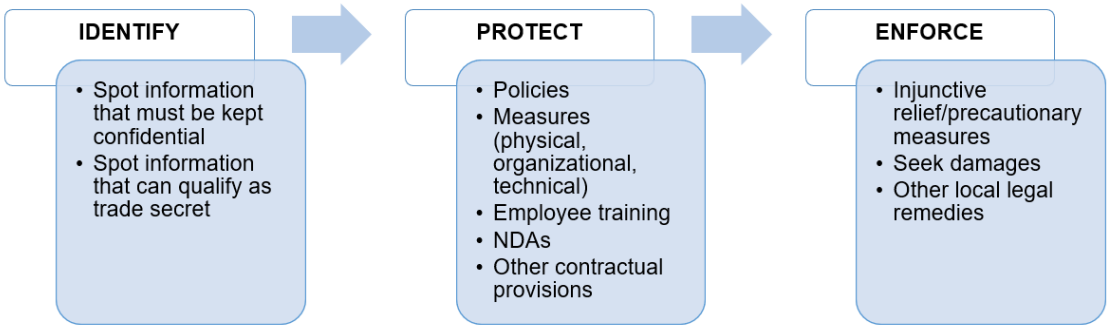
Before proceeding, we recommend a rereading of trade secret protection in chapter 4, and NDAs in chapter 5 and earlier in this chapter, which will provide a foundation for understanding the subsequent content.[46]

Information that is both secret and holds commercial value can – and should – be safeguarded as a trade secret. NDAs serve as a contractual means to protect confidential information and trade secrets when sharing them with other entities. Safeguarding and enforcing trade secrets, however, entails more than just NDAs.

The life of a trade secret and confidential information can be separated into three phases.

[46] See World Intellectual Property Organization. The Role of Intellectual Property Rights in the Development and Commercialization of Mobile Applications. WIPO, 2021: chapt. 2.2.

Figure 10.8 The trade secrets life cycle



Source: the authors.

The first step is identification. Once you have identified the pieces of information that give you a market advantage over competitors or hold commercial value (for example, the idea underlying your app, details of its features and technical functionalities, financing or monetization strategies), there are different actions that can be taken to make the rights effective and enforceable in cases of infringement, including:

1. **Create confidentiality and/or trade secret policy**: creating and implementing a policy is the first step to ensure a uniform approach within your company, thereby safeguarding confidential information in a consistent manner. The policy should outline, at a minimum, how to identify confidential information, methods to protect it, applicable measures, authorized access, and circumstances under which sharing information with other entities is permissible.
2. **Train your employees**: to maximize the policy's effectiveness, it is advisable to regularly train employees on its contents. Merely having staff members sign the policy is insufficient as only a few will likely read it.
3. **Prepare an NDA template adapted to specific situations**: seeking legal counsel for drafting an adaptable NDA template is recommended for instances when you need to

share confidential information with third parties. Scenarios where sharing might be necessary include:

- partnerships or collaborations requiring disclosure of marketing plans or app details;
- engagement with external developers needing access to existing source code or preliminary documents; and
- potential investors reviewing business and financial plans.

4. **Protect confidential information and trade secrets in the workplace**: employees pose a potential risk of unauthorized use and disclosure of your trade secrets and confidential information. Consider the possibility of former employees stealing valuable information to create a competing app or business, or disloyal employees selling your information to competitors. Include specific provisions in employment contracts concerning confidentiality obligations, along with a reference to the confidentiality policy every employee must sign.
5. **Legal enforcement of your rights against infringement**: depending on the country where you operate or the infringement occurs, you are entitled to take action. It is advisable to consult a local lawyer on the available actions. Generally, your options include injunctive relief/precautionary measures, seeking damages and, in certain countries, treating unauthorized access and/or use of third-party confidential information and/or trade secrets as a criminal offense.

Case study: Tinder's lawsuits against competitors

Background

Tinder is a widely used dating application offered by Match Group, whose name and logo is known worldwide. The company sued two different competitors:

1. 3nder (now Feeld), a mobile app in the dating sector whose name sounded extremely similar to Tinder.

2. Muzz (formerly Muzmatch), the world's largest Muslim dating app whose trademark and part of its GUIs resemble Tinder's.

The claim against 3nder

Tinder noticed that the competing app had a similar name, and in May 2016, Match Group threatened 3nder with a trademark lawsuit. After this, in August 2016, 3nder changed its name to Feeld.

The claim against Muzz

Match Group twice sued the company behind Muzz. First, in the United Kingdom, for trademark infringement, and second, in the United States of America, for patent and trademark infringement, unfair competition and false designation of origin.

Tinder won in the United Kingdom, where Muzmatch was forced to rebrand to Muzz. It is worth noting that Muzz declared spending 2 million US dollars in legal fees due to the claims received.

Comments

These cases show the importance of registering IP rights in order to enforce them, and of periodically monitoring any unauthorized use of your IP assets or infringement of your IP rights. They also emphasize the importance of ensuring your app does not infringe any third-party IP rights, as the consequences can include not only changing the app's name, aesthetic or operations, but also bearing the high cost of legal fees.

Checklist: protect your IP rights

- Identify assets that can be protected by IP rights.
- Register rights that require registration and consider registering copyrights for easier enforcement.
- Contractually protect your rights, including specific wording in your app's terms.
- Monitor unauthorized use of your IP.
- If any infringement is detected, enforce your rights, via:
    - informal contact;
    - cease and desist letter;
    - negotiate a license, if possible;
    - try to agree on an ADR mechanism; or

- file a lawsuit.

- Along the life of your app, identify trade secrets and confidential information and protect them:
  - create a confidentiality policy;
  - enter into NDAs and confidentiality obligations with external entities and employees;
  - train employees on confidentiality; and
  - enforce your rights in case of infringement.

Enforcement and professional associations

When it comes to enforcing IP rights, professional associations play an important role, from ongoing training and outreach aimed at identifying and registering IP, to supporting and making available ADR mechanisms. For a comprehensive understanding of the functions of professional associations, see chapter 11.

10.5. Conclusions

Respect for IP rights is essential for all parties involved in the app ecosystem: from agencies who develop code and content for the app owner, and the app owner in designing and publishing the app and including content and other materials, to business clients and end users who download and use the app.

For the app owner, compliance with third-party IP is not just an ethical must, it is also contractually warranted by the app owner in the app store contract, and it may have to indemnify the store against any loss or damage it suffers due to an infringing app. App stores are also key in enforcing rights, as an IP holder may address a claim to the store requesting the withdrawal or suspension of the publication of an infringing app.

Accordingly, carrying out due diligence and verification processes are a useful and practical means to ensure compliance.

Key takeaways

- Mobile app development and commercialization often involves using third-party works protected by their IP rights.
- Establish due diligence steps to 'clear' third-party rights, from patent freedom to operate and trademark searches, to verification with employees and third-party developers.
- Obtain appropriate licenses to such third-party materials and comply with license obligations (especially open source and content).
- Include contractual protection clauses in app development contracts to ensure developers are aware of and comply with IP compliance requirements.
- Pay particular attention to the use of confidential information and data.
- Protect your own IP through identification, registration (when relevant), and marking (for example, using the © and ™ signs).
- Ensure proper evidence of rights so you can support claims of breach if need be.
- Monitor the market (online, through specialist service providers) for abuse of your IP and be proactive in policing/enforcing it.
- Seek professional advice from IP specialists for compliance and enforcement.

10.6. Useful links and resources

WIPO, *The Role of Intellectual Property Rights in the Development and Commercialization of Mobile Applications*.

Chapter 11. The role of professional organizations

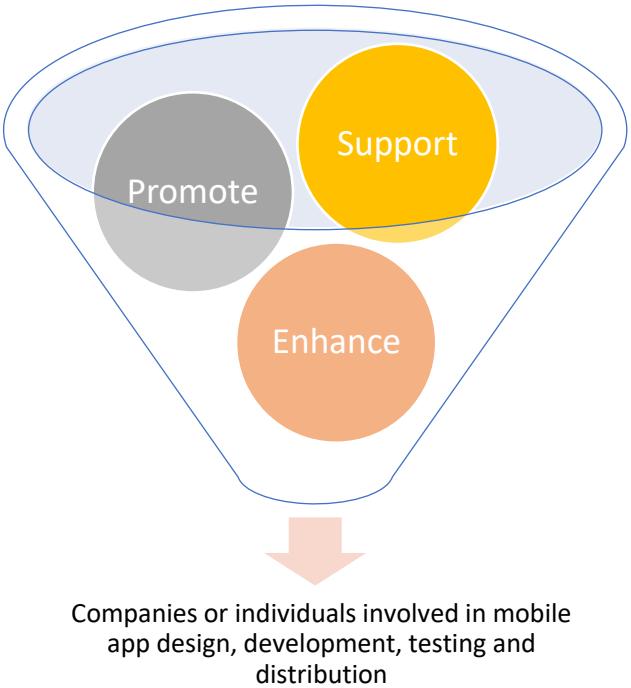
11.1. Introduction

This chapter looks at the role of professional organizations in the context of mobile apps. Such organizations are significant, acting as the industry backbone and providing a structured, standardized and ethical environment for growth. They bridge the gap between individual developers, businesses and the global marketplace, ensuring the smooth flow of innovation, commerce and knowledge.

11.2. The many roles of professional organizations

The professional organization is an association or group that serves the needs of app owners, developers, agencies and individuals or companies involved in mobile app design, development, testing and distribution. Such organizations aim to support, promote and enhance the professional growth and interests of their members.

Figure 11.1 Roles of mobile apps sector professional organizations



Source: the authors.

As mobile apps transcend national borders and weave themselves into the fabric of global digital activities, the role of professional organizations in steering their progress becomes increasingly necessary. Many app owners and developers are small and medium enterprises (SMEs), and lack the knowledge or power to influence evolution of the sector. With industry-specific understanding of mobile apps and the technology per se, professional organizations are able to significantly influence policies that impact the industry.

This chapter outlines the multifaceted roles such organizations play within the international mobile app ecosystem, as follows:

- **Knowledge sharing and resources**: often offer resources, publications and educational materials related to mobile app development and commercialization. Organizations can provide access to industry reports, case studies, white papers and research findings, helping professionals stay updated on trends, technologies and insights.
- **Networking and collaboration**: provide a space for app owners, developers, designers, marketers and other industry professionals to connect, network and collaborate. Organizations promote events, conferences and meetings where people can share knowledge, ideas and best practices.
- **Advocacy and representation**: advocate for the interests and needs of the mobile app sector. They represent the industry in discussions with policymakers, regulatory bodies and other stakeholders. By voicing concerns, proposing policies and influencing decision-making, they contribute to shaping a favorable environment for mobile app development and entrepreneurship.
- **Standards and best practices**: may establish and promote industry standards and best practices for mobile app development. By developing guidelines related to user

experience, security, privacy, accessibility and other crucial aspects, professional organizations enhance professionalism, quality and user trust within the industry.

- **Professional development and training**: offer professional development programs, training courses, certifications and workshops. Such initiatives may help app owners, developers or agencies to enhance their skills, expand their knowledge and stay competitive in the rapidly evolving mobile app sector.
- **Industry research and insights**: conduct research, surveys and studies to gather insights into market trends, user behavior and industry challenges. Findings contribute to a better understanding of the sector and help professionals make informed decisions.

The App Association

The App Association focuses its efforts on the opportunities and challenges faced by SMEs operating as app owners and/or developers in the app ecosystem today. Among its many activities, APC focuses on three core pillars.

Advocacy

The App Association connects app owners and developers directly with the policymakers who affect their business, through letter-writing campaigns, petitions, briefings for political staff and in-person meetings. The App Association purpose is to educate policymakers on the possible consequences and impact of potential legislation on small, technology-based businesses, and to provide support for better policies and regulations. The App Association also works to amplify the small business perspective in policy debates at local, federal and international levels, and connects members with media outlets around the world looking to hear directly from innovators in the app economy.

The App Association is currently focusing its efforts on policy development in the areas of:

- privacy, given its global impact and complexity;
- competition and antitrust (for example, the relationship between platforms and mobile apps);
- IP issues relating to access and use of standard essential patents;
- global economic issues, such as tax codes and changes in fiscal incentives; and

- new technologies, such as the regulation of AI in the mobile app sector.

The App Association is also concentrating on developing nations in Southeast Asia, the Caribbean (for example, Trinidad and Tobago) and other regions to facilitate a positive policy environment for the start-up community in these countries.

Community

The App Association builds community among its members by connecting them through events that highlight emerging technology hubs, and by helping educate application developers and innovators at all stages. They also facilitate connecting with expert industry partners for business and strategy guidance.

Resources

The App Association provides a repository on its website with resources on intellectual property or third-party tools, where they give relevance to important policy issues as well as report on market trends around the world through newsletters, social channels and events.

The App Association: https://actonline.org/eu/

11.3. Relevant mobile apps professional organizations

We have compiled a list of the most relevant professional organizations in the mobile app sector by territory.

Table 11.1 Professional organizations, territories where present and description of activities

Professional organization	Territory	Description
ACT, The App Association	Worldwide, mainly North America, United Kingdom, Europe	Global trade membership organization for SME technology companies and software developers.
Developers Alliance (DA)	North America	Nonprofit global membership organization that supports app owners, developers and other key players in the technical and business challenges of app development and distribution.

International Game Developers Association (IGDA)	Worldwide	Nonprofit global membership organization for app owners, developers and other key players.
GSMA	Worldwide	Represents the interests of mobile operators, including app owners and developers, encompassing some 800 operators with almost 300 companies in the broader mobile ecosystem.
Mobile Marketing Association (MMA)	Worldwide	Focuses on establishing mobile as an indispensable part of the marketing mix. Offers resources, research and guidelines related to mobile advertising and marketing.
International Federation for Information Processing (IFIP)	Worldwide	Focuses on information processing and communication technologies. Have working groups and conferences related to mobile app development and research.
MobileMonday	North America	Global community of mobile industry professionals, as app owners, developers and other key players with active chapters in various European cities and elsewhere. Organize regular events and gatherings, providing a platform for networking and knowledge sharing.
Interactive Advertising Bureau (IAB)	North America	While not exclusively for mobile apps, IAB offers significant resources and insights into mobile advertising and marketing.
European Mobile Media Association (EMMA)	Europe	Represents the interests of the messaging industry in Europe
Mobile Ecosystem Forum (MEF)	Europe, Asia, Africa	Global trade body that addresses the key issues facing the mobile ecosystem.
Mobile Marketing Association - Asia Pacific	Asia	Focuses on promoting and enhancing mobile marketing and its associated technologies in the Asia Pacific region.
Wireless Application Service Providers'	Africa	Based in South Africa and provides a framework for self-regulation for mobile application service providers in the region.

Association (WASPA)		

Source: the authors.

Example of professional organization activity

Charlotte, an app owner, recently launched health and fitness app FitZone in app stores. It rapidly gained popularity, attracting a substantial user base within a few months of its release. However, an issue arose when a well-known tech blogger claimed that FitZone had a feature that accessed a user's personal contact data without their knowledge or permission. The controversy quickly spread across social media and tech forums, leading to a significant public relations crisis for Charlotte.

The negative publicity around the mobile app led to a decrease in its download rates, and several users started uninstalling it. Charlotte's reputation as a trustworthy app owner was at stake, and she faced potential legal repercussions if the allegations were found to be true. Accessing user data without permission can lead to hefty fines and lawsuits.

Charlotte reached out to a well-regarded professional organization in the mobile sector (hereafter MDA) for assistance and the following services were made available to her:

- **Legal guidance**: MDA's legal team provided Charlotte with guidance on the legal aspects of data privacy and user consent. They helped her understand her rights and obligations as a developer and suggested enhancements in the app's privacy policy and terms of service.
- **Technical assessment**: with Charlotte's consent, MDA carried out an independent technical audit of the mobile app. It was found that while FitZone did have a feature requesting access to contacts, it was for a social sharing feature and was transparently presented to users during the setup. The claim was a result of misunderstanding and lack of clear communication on Charlotte's part about the mobile app's features.
- **Public relations support**: with guidance from MDA, Charlotte launched a transparency campaign addressing the controversy head-on. She released a detailed statement clarifying the app's functionalities, the results of the independent audit, and the steps she would take to enhance user trust.

- **Educational workshops**: Charlotte attended MDA workshops on mobile app development ethics, data privacy and user-centric design, which enhanced her understanding and ensured she would not face such problems in the future.

Outcome

With MDA's support, Charlotte managed to navigate the crisis effectively. The controversy was addressed, and FitZone's reputation started to recover. Charlotte also implemented a feedback mechanism within the app, allowing users to communicate their concerns directly.

11.4. The benefits of joining a professional organization

A professional organization offers a series of benefits tailored to the unique needs and challenges that app owners and developers face in the current digital landscape.

It grants developers access to a store of resources and tools, often curated by industry veterans, which can significantly streamline the app development process. Organizations frequently provide exclusive research, insights and state-of-the-art tools that equip developers with the knowledge and technologies to keep their applications cutting edge. This can prove invaluable, especially in a domain where being up to date is not a luxury but a necessity.

Figure 11.2 Benefits of professional organizations in the mobile app sector

Source: the authors.

Further, such affiliation can provide credibility and boost professional standing in the competitive app market. Being a member of a recognized organization often acts as a stamp of trust and quality, signaling to clients, peers and users that one's app adheres to industry standards and best practices. Additionally, these organizations offer interesting networking opportunities.

The connections that app developers forge with industry peers, potential clients and even mentors can open doors to collaborative projects and job opportunities, and provide a platform for the exchange of ideas and knowledge, nurturing both individual growth and the collective advancement of the mobile app development community.

The International Game Developers Association

The International Game Developers Association (IGDA) makes special interest groups available to its members. Such groups consist of global communities led by volunteer advocates. There are different groupings categorized as advocacy (focused on advocacy or social issues), discipline (game development) and affinity (helping game developers with

similar backgrounds or interests get in touch with each other) through which volunteers can share issues related to the mobile app sector.

For example, the IGDA Women in Games (WIG) Special Interest Group (SIG) encourages a positive impact on the game industry with regard to gender balance at work and in the marketplace.

Source: International Game Developers Association at https://igda.org/

11.5. App owners contributions to the ecosystem through professional organizations

In addition to the benefits that membership of professional organizations brings, app owners can also make a relevant contribution to the mobile industry through such organizations, including:

- **Policy impact and contribution**: the expertise and credibility of app owner and developer members enable effective advocacy for policies that benefit them, which allows them to leverage their participation in advocacy initiatives via professional organizations. This makes it possible for professional organizations to contribute to the endorsement of letters to legislators or to engage in direct discussions with legislators and policymakers.
- **Thought leadership**: given their hands-on experience, app owners and developers can provide insights into emerging trends, best practices and upcoming challenges. They can be invited to write articles, present webinars or speak at conferences, enlightening peers with their experiences and vision.
- **Technical workshops and training**: app owners can host workshops teaching specific skills, such as using a new framework, implementing best practices in app security, or understanding the nuances of user interface/user experience (UI/UX) design. This helps raise the overall skill level within the organization.

- **Beta testing and feedback**: app owners can offer their mobile apps as case studies for beta testing, allowing peers to provide feedback. This collaborative approach helps identify issues, improve app quality and foster a sense of community.
- **Open source contributions**: app owners may contribute to open source projects, introducing and encouraging the adoption of open source tools within the professional organization, leading to better and more robust applications.
- **Mentorship**: senior or more experienced app owners can provide mentorship to budding app creators, which helps in skill transfer and also fosters a supportive environment within the professional organization.
- **Resource sharing**: app owners often benefit from resources such as articles, tools and courses, and sharing these within the organization can aid collective growth. [47]
- **Industry representation**: app owners can represent the professional organization at other industry events, promoting its goals, values and standards. Such representation ensures that the voice of the owner community is heard and considered in broader tech or policy discussions.
- **Feedback loop creation**: given their close interaction with end users, app owners can provide direct feedback to hardware manufacturers, developers and other stakeholders about device performance, OS limitations or other technical issues that affect app performance.
- **Collaborative projects**: app owners can spearhead collaborative projects where members of the organization work together to create mobile apps, tackle challenges or explore new technological frontiers.
- **Ethical advocacy**: app owners play a pivotal role in highlighting and advocating for ethical considerations in app development, such as user privacy, data security and

[47] See ACT – The App Association, *Licensing Guide*: www.actonline.org/wp-content/uploads/2018_ACT-Licensing-Guide_May1.pdf. (last visited March 2024)

inclusivity. Their voice can guide the organization in creating guidelines and best practices that uphold these values.

The Developers Alliance

Developers Alliance (DA) provides access to the Developer Policy Network available on its website.[a] If the app owner decides to sign up, DA may occasionally ask them to consider signing a letter to legislators or speaking directly to a legislator. Lately, DA in the United States of America has been repeated in the negotiation process of public policies, related, for example, to the AI Accountability Policy Request for Comment.[b] It states that "a plurality of app developers (36 per cent) believe software associations should serve as the chief regulators of the industry with fewer supporting government or agency regulation".

More information is available on the Developers Alliance website, http://www.developersalliance.org/us-software-developers-are-engaged-on-public-policy-infographic/.

[a] Online at https://developersalliance.org/

[b] Regulations.gov. "Comment on FR Doc # 2023-07776. *regulations.gov*. Jun. 15, 2023. <www.regulations.gov/comment/NTIA-2023-0005-0791>.

11.6. Conclusions

The mobile app ecosystem is vast, evolving and influenced by countless variables. An app owner is not only determined by the code they write but also by their understanding of industry trends, the relationships they cultivate and the quest for knowledge and innovation. Professional organizations have emerged as anchors in this vast sea, providing guidance, support and a myriad of opportunities for app owners and developers worldwide.

Joining a professional organization offers many benefits. It allows app owners and developers to connect with like-minded peers, fostering collaboration and potentially leading to groundbreaking innovations. Such organizations often serve as the first point of information for industry standards, best practices and changing market dynamics. The resources, be it in the form of seminars, workshops or courses, are invaluable for app owners/developers'

continuous growth. Moreover, the credibility and validation these organizations provide can enhance professional stature, opening doors to opportunities that might otherwise remain elusive.

The relationship is not just one-sided. By becoming active participants in these organizations, app owners and developers contribute immensely to the mobile ecosystem. App developers bring real-world experiences, challenges and insights, helping to shape the industry's future. When app owners and developers share knowledge, advocate for policy change or collaboratively find solutions to common hurdles, the entire mobile community benefits. This symbiotic relationship ensures the ecosystem remains vibrant, innovative and responsive to the changing needs of its user base.

In conclusion, mobile app professional organizations are more than just platforms for networking or skill enhancement. They are pivotal to balancing individual growth (for app owners) and collective progress (for the sector and society). For app owners, engaging actively with such organizations is not just a pathway to personal success but also an opportunity to contribute meaningfully to an industry that touches billions of lives daily. As the mobile app landscape continues to evolve, these organizations, together with their member app owners and developers, will undoubtedly continue to play a central role in sculpting the digital future.

Key takeaways

- Professional organizations play a key role in the mobile app industry.
- You can participate in legislative consultation and policy development processes to ensure your interests are reflected in them.
- You can seek technical and legal guidance from professional organizations as well as gain access to useful tools such as publications, research, events and conferences.

- By belonging to a professional organization, you can learn from the experience of other key players in the sector and improve your business strategy and product development.

11.7. Useful links and resources

More information is available on the organizations' websites:

ACT – The App Association. https://actonline.org/uk/
Application Developers Alliance (DA): https://developersalliance.org/
GSMA. https://www.gsma.com/
Mobile Marketing Association (MMA). http://www.mmaglobal.com/
International Federation for Information Processing (IFIP). http://www.ifip.org/homeintro.html
MobileMonday. http://www.mobilemonday.us/
Interactive Advertising Bureau (IAB). http://www.iab.com/
European Mobile Mobile Association (EMMA). http://www.emmanet.com/indexold.html
Mobile Ecosystem Forum (MEF). http://www.mobileecosystemforum.com/
Mobile Marketing Association Asia Pacific (MMA) www.mmaglobal.com/documents/state-mobile-marketing-asia-pacific
Wireless Application Service Providers' Association (WASPA). http://www.waspa.org.za/
International Game Developers Association at https://igda.org/

About the authors

Malcolm Bain

Malcolm Bain is partner for information technology and IP law at Across Legal law firm, Barcelona, as well as associate professor at the University of Barcelona. He has worked for 25 years in the field of ICT law, being a solicitor in England and abogado in Spain. He is a guest lecturer at several universities and national and international events, and has been invited to speak at WIPO-organized events on several occasions.

Lucrezia Berto

Lucrezia Berto is an associate in Across Legal's IP and information technology department. She holds an LLM in Law of Internet Technology from Bocconi University, Italy, and specializes in noncontentious IP and IT matters, such as software licensing, open source software, e-commerce, privacy and IT contracts.

Marcelo Estrella Orrego

Marcelo Estrella is an associate in information technology law, IP and personal data protection at Across Legal, Barcelona. He has worked for five years in ICT law, being an abogado in Argentina and an industrial property agent. He has collaborated with several companies, both nationally and internationally. Marcelo has also worked with several universities, focusing on technology transfer offices.

Beatriz Benítez-Alahija

Beatriz Benítez-Alahija is a Spanish-qualified associate lawyer for information technology and IP law at Across Legal in Madrid and Barcelona. She has been advising technology-based companies for more than five years, as well as public institutions, nationally and internationally, on issues related to IP, new technologies and privacy.

Acknowledgements

We are grateful to WIPO for the opportunity to prepare this material, which we hope will be useful in the mobile app ecosystem, and for the suggestions and guidance of Dimiter Gantchev. We would also like to thank the authors included in the bibliographical references of this handbook, especially Andrew Katz and Noam Shemtov.