

# RESEARCH ON BUSINESS MODELS INFRINGING INTELLECTUAL PROPERTY

Phase 6: Applications Related to Serious  
and Organised Intellectual Property Crime



# RESEARCH ON BUSINESS MODELS INFRINGING INTELLECTUAL PROPERTY

Phase 6: Applications Related to Serious and  
Organised Intellectual Property Crime

Catalogue number: TB-02-24-684-EN-N ISBN: 978-92-9156-359-3 DOI: 10.2814/09772  
© European Union Intellectual Property Office, 2024  
Reuse is allowed provided the source is acknowledged and changes are mentioned (CC BY 4.0)

## Table of contents

<b>Acknowledgments</b> .....	<b>6</b>
<b>Disclaimers</b> .....	<b>7</b>
<b>How to read the report</b> .....	<b>8</b>
<b>Call for contributions</b> .....	<b>9</b>
<b>List of items (text boxes, tables, and figures)</b> .....	<b>10</b>
<b>Foreword</b> .....	<b>12</b>
<b>Executive summary</b> .....	<b>13</b>
<b>Definitions</b> .....	<b>23</b>
<b>I Background, scope, and methodology</b> .....	<b>26</b>
<b>I.A Background</b> .....	<b>26</b>
<b>I.B Scope</b> .....	<b>28</b>
<b>I.C Methodology</b> .....	<b>29</b>
<b>I.C.1 Research deliverables</b> .....	<b>29</b>
<b>I.C.2 The arc of IP crime related to apps</b> .....	<b>30</b>
<b>I.C.3 Analysis of collected data</b> .....	<b>33</b>
<b>I.C.4 Structure of the report</b> .....	<b>33</b>
<b>II App ecosystem</b> .....	<b>41</b>
<b>II.A History of apps</b> .....	<b>41</b>
<b>II.B Widespread acceptance of apps</b> .....	<b>43</b>
<b>II.C Exploitation of IP in app development</b> .....	<b>46</b>
<b>II.D Developing and disseminating apps</b> .....	<b>47</b>
<b>II.D.1 Developing legitimate apps</b> .....	<b>47</b>
<b>II.D.2 Developing IP-infringing apps</b> .....	<b>52</b>
<b>II.D.3 App gateways</b> .....	<b>54</b>
<b>II.E Risks and harm</b> .....	<b>56</b>
<b>III Infringing business model 1: infringement of copyright-protected digital content</b> .....	<b>59</b>
<b>III.A Scheme and technical setup</b> .....	<b>60</b>
<b>III.A.1 Platform</b> .....	<b>60</b>
<b>III.A.2 Development</b> .....	<b>62</b>

III.A.3	Functionality .....	66
<b>III.B</b>	<b>Key enablers: gateways .....</b>	<b>69</b>
III.B.1	App stores, app marketplaces and other app brokers .....	70
III.B.2	Direct downloads and unauthorised downloads .....	71
<b>III.C</b>	<b>Execution and value capture .....</b>	<b>72</b>
III.C.1	Use .....	72
III.C.2	IP crime .....	73
III.C.3	Criminal gain .....	74
<b>IV</b>	<b>Infringing business model 2: marketing of IP-infringing physical goods.....</b>	<b>84</b>
<b>IV.A</b>	<b>Scheme and technical setup.....</b>	<b>85</b>
IV.A.1	Platform .....	85
IV.A.2	Development .....	85
IV.A.3	Functionality .....	85
<b>IV.B</b>	<b>Key enablers: gateways .....</b>	<b>88</b>
<b>IV.C</b>	<b>Execution and value capture .....</b>	<b>88</b>
IV.C.1	Use .....	88
IV.C.2	IP crime.....	89
IV.C.3	Criminal gain.....	96
<b>V</b>	<b>Infringing business model 3: IP infringement for malicious and fraudulent purposes .....</b>	<b>97</b>
<b>V.A</b>	<b>Scheme and technical setup.....</b>	<b>98</b>
V.A.1	Platform .....	99
V.A.2	Development .....	100
V.A.3	Functionality .....	100
<b>V.B</b>	<b>Key enablers: gateways .....</b>	<b>105</b>
<b>V.C</b>	<b>Execution and value capture .....</b>	<b>105</b>
V.C.1	Use .....	105
V.C.2	IP crime.....	106
V.C.3	Criminal gain.....	115
<b>VI</b>	<b>Infringing business model 4: trade secret theft .....</b>	<b>117</b>
<b>VI.A</b>	<b>Scheme and technical setup.....</b>	<b>119</b>
VI.A.1	Platform.....	120

VI.A.2	Development .....	120
VI.A.3	Functionality .....	121
VI.B	Key enablers: gateways .....	121
VI.C	Execution and value capture .....	122
VI.C.1	Use .....	122
VI.C.2	IP crime.....	122
VI.C.3	Criminal gain.....	126
VII	Perspectives and conclusions.....	127

## Acknowledgments



This report was developed thanks to the invaluable insights of a number of experts, including:

Alexander Velev, Andrii Shalaginov, Ankit Sahni, Benjamin Winsner, Bodgan Ciñaru, Constantin Rehaag, Cristopher C., Dani Bacsa, Dave Lowe, Didier Wang, Edyta Bednarczyk, Erling Vestergaard, Erwin Van Uffel, Graeme Grant, John Phelan, John Zacharia, Jure Kralj, Knud Wallberg, Lauren Arnold, Laurentiu Apostolescu, Lee Kent, Maria Fredenslund, Melissa Morgia, Michael Lund, Oliver Pribramsky, Pascal Hetzscholdt, Peter G Szyszko, Rob Pinniger, Stephan Edelbroich, Tara Amine, Vasilis Katos, Xavier Koehoorn, and Yulia K.

## Disclaimers

The views expressed in this report cannot be attributed directly to any interviewed or contributing expert. Moreover, not all of the experts may agree with all, or some of the views expressed in this report. The views expressed by any of the contributing experts do not represent the official position of the EUIPO. All quotes are edited and simplified extracts from expert interviews and anonymised for any identifiable information as to affiliation, geography, and any other specific information.

The content provided in this report constitutes a simplified and structured elucidation of the subject matter, emphasising overarching concepts rather than delving into exhaustive technical intricacies of applications. The report's primary objective is to underscore significant facets of the application ecosystem as they pertain to intellectual property crime, to the benefit of policymakers, civil society, academia, private businesses, IP practitioners, law enforcement authorities, and the judiciary. The information gathered by the provider of the study – predominantly consisting of practitioner interviews – is not intended to be exhaustive in terms of concepts, examples, technical descriptions and detail, and, due to nature of the subject matter, some aspects might overlap in different sections of the report, reflecting the interconnected nature of the topics discussed.

This report is not intended to give legal advice and neither supersedes, nor substitutes, the requirements of national law, international law, or any government regulations, policies, or priorities.

## How to read the report



The report is designed with flexibility in mind as each chapter is intended to be self-contained rather than read from cover to cover. To facilitate easy navigation, the report includes clickable cross-references. By clicking on the section number, the reader is taken directly to the information they are looking for.

For a comprehensive understanding, it is advisable to begin with the executive summary, which provides an overview of the key findings and insights. Additionally, it is recommended to read the perspectives and conclusion chapter for a full scope of the implications and overarching themes of the report.



## Call for contributions



The EUIPO welcomes any suggestions or ideas that could add to or improve the fight against intellectual property crime. If you would like to comment or contribute, please send an email to:

[observatory@euipo.europa.eu](mailto:observatory@euipo.europa.eu)

## List of items (text boxes, tables, and figures)

Item 1. <b>The arc of IP crime related to apps</b> .....	15
Item 2. <b>The four business models</b> .....	16
Item 3. <b>Nine important emerging trends</b> .....	19
Item 4. <b>Nine enforcement and investigative measures</b> .....	21
Item 5. <b>Six law enforcement investigative strategies</b> .....	22
Item 6. <b>The four business models</b> .....	31
Item 7. <b>The arc of IP crime related to apps</b> .....	32
Item 8. <b>The structure of the first chapter of the report</b> .....	34
Item 9. <b>Overview of case examples</b> .....	36
Item 10. <b>Nine important emerging trends</b> .....	37
Item 11. <b>Nine enforcement and investigative measures</b> .....	39
Item 12. <b>Mobile app evolution timeline</b> .....	42
Item 13. <b>Apps entering the business world</b> .....	45
Item 14. <b>Life cycle phases of an app</b> .....	46
<b>Item 15. Life cycle phases of an app with the 7 steps of development</b> .....	47
Item 16. <b>7-step process for app development</b> .....	48
Item 17. <b>Actors involved in app development</b> .....	51
Item 18. <b>Criminal-infiltrated 7-step process for app development</b> .....	52
Item 19. <b>Important emerging trend – artificial intelligence (AI)</b> .....	53
Item 20. <b>Risks and harms of IP crime</b> .....	56
Item 21. <b>Enforcement and investigative measure – criminal referrals</b> .....	58
Item 22. <b>The arc of IP crime related to apps</b> .....	59
Item 23. <b>Case example - App piracy group</b> .....	61
Item 24. <b>Important emerging trend – dark web</b> .....	62
Item 25. <b>Important emerging trend – crime-as-a-service (CaaS)</b> .....	64
Item 26. <b>Enforcement and investigative measure – reverse engineering</b> .....	66
Item 27. <b>Case example – Xtream codes</b> .....	68
Item 28. <b>Enforcement and investigative measure – cooperation with app stores</b> .....	71
Item 29. <b>Enforcement and investigative measure – MICE framework</b> .....	74
Item 30. <b>Important emerging trend – digital display advertising</b> .....	76
Item 31. <b>Enforcement and investigative measure – cryptocurrency forensics</b> .....	78
Item 32. <b>Case example – Popcorn time application</b> .....	79

Item 33. Important emerging trend – social media and encrypted instant messaging apps.....	81
Item 34. Case example - Mobdro .....	82
Item 35. Law enforcement investigative strategies relevant to infringement of copyright-protected digital content.....	83
Item 36. The arc of IP crime related to apps .....	84
Item 37. Important emerging trend – versioning .....	86
Item 38. Primary provenance for IP-infringing products .....	92
Item 39. Different apps with varying functions v one superapp covering all listed functions .....	94
Item 40. Important emerging trend – superapps .....	95
Item 41. Law enforcement investigative strategies relevant to marketing of IP-infringing goods .....	96
Item 42. Enforcement and investigative measure – financial investigation .....	97
Item 43. The arc of IP crime related to apps .....	98
Item 44. Important emerging trend – geo-blocking .....	104
Item 45. Enforcement and investigative measure – raising awareness .....	106
Item 46. DNS abuse .....	108
Item 47. Enforcement and investigative measure – internet investigation.....	109
Item 48. Law enforcement investigative strategies relevant to IP infringement for malicious and fraudulent purposes .....	115
Item 49. Important emerging trend – cryptocurrencies .....	117
Item 50. The arc of IP crime related to apps .....	119
Item 51. Enforcement and investigative measure – collection and handling of electronic evidence.....	120
Item 52. Case example – Waymo v. Uber .....	123
Item 53. Law enforcement investigative strategies relevant to trade secret theft .....	124
Item 54. Law enforcement investigative strategies relevant to trade secret theft .....	126
Item 55. The arc of IP crime related to apps .....	128
Item 56. Techniques used for criminal purposes .....	130
Item 57. Revenue sources.....	133
Item 58. Enforcement and investigative approaches .....	135

## Foreword

In 2012, the Observatory on Infringements of Intellectual Property Rights ('the Observatory') was entrusted to the EUIPO to provide facts and evidence to support effective intellectual property (IP) policies, create tools and resources to aid in the fight against IP infringements, and raise awareness of the importance of IP and the negative effects of IP infringement.

One of the Observatory's main focuses during the past 12 years has been to understand how IP criminals conduct their illegal business. The infringing business model studies that began in 2016 have now reached their 6th edition and are among the main tools to enhance our understanding of IP-infringing business models and thereby provide a basis for identifying possible responses to effectively tackle this challenge.

This edition of the report provides a clear overview of the threats to IP from apps. The report comes with examples ranging from sales of counterfeits and copyright piracy to IP infringement-facilitated fraud and theft of trade secrets. The report also outlines how the misuse of apps poses new challenges for enforcement and investigations.

The risks and damages of IP infringement using apps mentioned above, and other criminal activities, emphasise how crucial it is to deal with and stop IP infringement effectively.

As we are in the middle of the European Union Serious and Organised Crime Threat Assessment (EU SOCTA) policy cycle 2022-2025, it is increasingly clear that IP crime poses serious threats to users, innovators, and creators, as well as small, medium-sized and large companies alike, and have grave economic consequences, both on a micro- and macro-economic level.

The results, insights and examples provided in this phase of the research series make a very compelling case for the need to maintain IP crime as an EMPACT priority in future policy cycles. This research is conducted with the aim of helping law enforcement, the judiciary, academia, the private sector, and policymakers in the fight against IP crime.

It is also noteworthy that on 19 March 2024 the Commission adopted a comprehensive set of recommendations to combat counterfeiting and protect IP, which included a number of actions to improve the criminal enforcement response to IP crime.



João Negrão

Executive Director

EUIPO



## Executive summary

### Background

The research study series on business models infringing intellectual property (IP) has, since 2016, been one of the initiatives of the Observatory on Infringements of Intellectual Property Rights ('the Observatory') entrusted to the EUIPO. This 6th edition in the series focuses on the criminal threats to IP related to applications ('apps').

The subject of apps has been selected for analysis because of their rapid expansion and wide acceptance by society, consumers, and internet users; technical developments; and the relevance of apps to the legal exploitation of IP, as well as overall app misuse by IP criminals.

The development of the study was entrusted to the Deloitte Advisory, S.L. group, focused on fraud prevention and financial crime matters, supported by the Observatory network.

### Methodology

This report is the first deliverable of the research study and is a result of the empirical and qualitative analysis conducted by the research team. It is based on:


- a literary review of existing studies and reports on the topic;
- an examination and analysis of relevant jurisprudence;
- two hands-on workshops conducted in early 2023 with members of the Observatory Impact of Technology expert group as well as public- and private-sector representatives;
- semi-structured interviews with leading IP experts with experience in infringements of IP related to apps;
- independent research on commercialisation, sharing and the use of apps that have an impact on the IP crime landscape.

The content provided in this report constitutes a simplified and structured elucidation of the subject matter, emphasising overarching concepts rather than delving into exhaustive technical intricacies of applications. The report's primary objective is to underscore significant facets of the application ecosystem as they pertain to IP crime, to the benefit of policy makers, private sector, IP practitioners, law enforcement and judiciary. The information gathered by the provider of the study – predominantly consisting of practitioner interviews – is not intended to be exhaustive in terms of concepts, examples, technical descriptions and detail, and, due to nature of the subject matter, some aspects might overlap in different sections of the report, reflecting the interconnected nature of the topics discussed.

The report will be followed by a collection of investigative practices and training materials for law enforcement and the judiciary. They will contribute to the Observatory's efforts to support the European Multi-disciplinary Platform against Criminal Threats (EMPACT), a security initiative driven by EU Member States to identify, prioritise and address threats posed by organised and serious international crime, in which IP crime is a dedicated priority (see Footnote 20).

The key findings of the report document the need for a robust criminal enforcement response to serious and organised IP crime, which is also in line with the recent Commission recommendations to combat counterfeiting and protect IP (see Footnote 21).

The report highlights that serious and organised criminals understand the intrinsic value of IP and exploit it for illegal gain. As such, IP owners facing significant and deliberate infringement, often at a commercial level, may turn to public authorities for criminal action. The supplementary 'Intellectual Property Owner Guide to Criminal Referrals in Intellectual Property Crime Cases' offers a guide for IP owners on referring such infringements for criminal investigation. Given the variation in national laws on criminal sanctions for IP crimes such as counterfeiting and copyright infringement, the forthcoming EUIPO study 'Legislative Measures Related to Intellectual Property infringements – Phase 3: Criminal Measures in Serious and Organised Intellectual Property Crime Cases,' set for mid-2024 release, will provide a detailed analysis of criminal measures against IP crime.



*Organised crime groups are increasingly behind app enabled IP crime and the security awareness amongst IP criminals is ever growing. The main enforcement task goes against the backbones of criminal organisations. We need an ever more united international effort to target and deal with this kind of organised crime.*

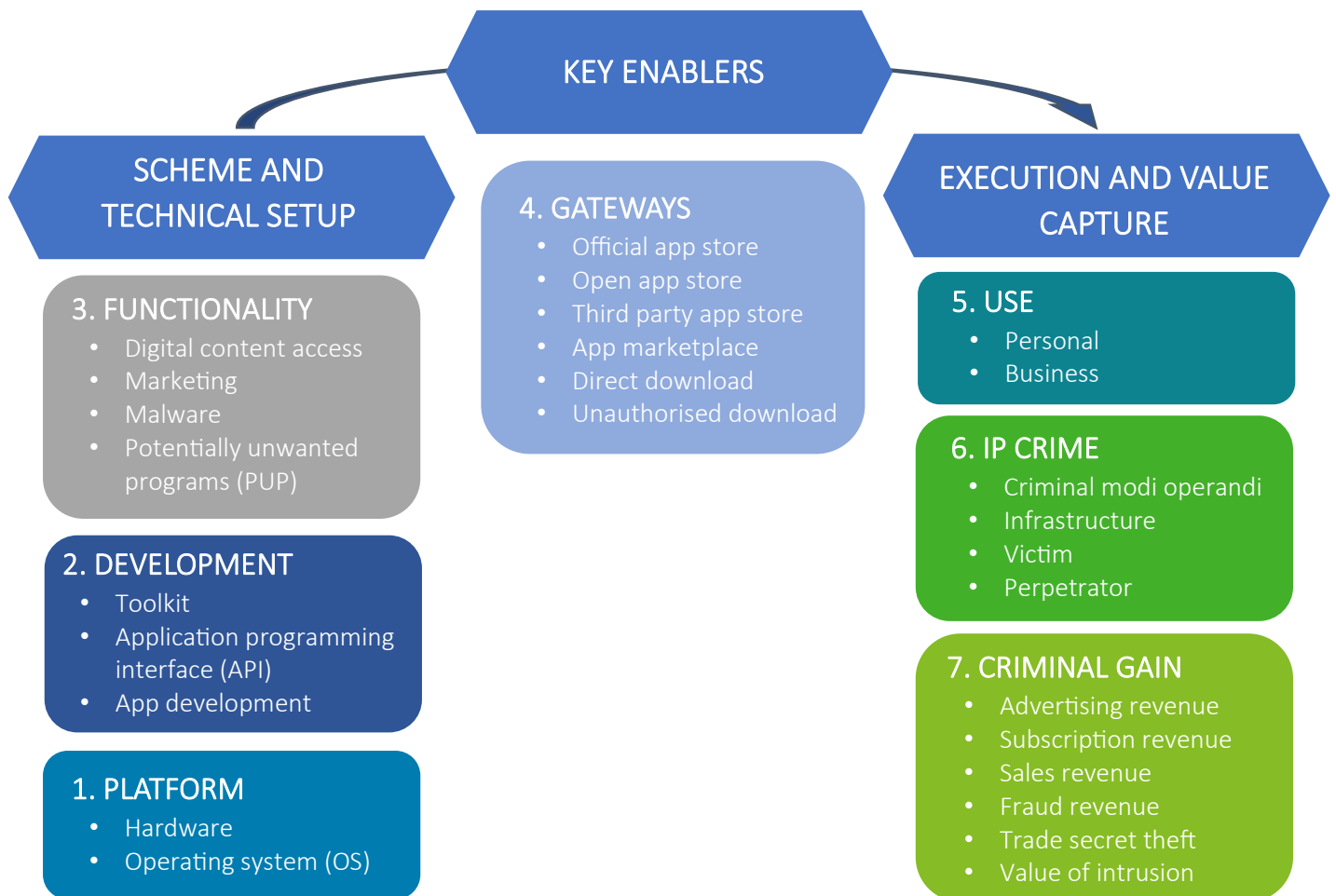
IP crime expert

The content of this report is complementary to the research led by the Observatory through the Cooperation with Intermediaries Expert Group on the misuse of Apps and App stores, focusing on how this ecosystem can be misused for intellectual property infringing activities, and how these misuses can be counteracted through good practices. A discussion paper on the topic will be published in parallel with this report.

***The arc of IP crime related to apps***

To support the analysis in this research study, a unique graphical model was created depicting seven key elements of app-related IP crime, named *the arc of IP crime related to apps*.

Item 1. ***The arc of IP crime related to apps***



*The arc of IP crime related to apps* focuses on three main elements divided into seven parts.

- The scheme and technical setup:
  - platform: technical environment in and for which an app is developed;
  - development: the methods that the app developers use to create the app;
  - functionality: the ultimate intended features of the application.
- The key enablers: gateways: the channel or channels on which the app is made available to users.

- The value capture and gain achieved by IP criminals:
  - Use: the practical use for the app’s target audience;
  - IP crime: the specific criminal elements in each of the four IP-infringing business models identified in this report;
  - criminal gain: the monetary or non-monetary advantage obtained by IP criminals.

On the basis of the *arc of app-related IP crime* and the data collected, a technical analysis of the types of apps used for IP-infringing activities was conducted, together with an analysis of the app ecosystem. Therefore, although all types of IP are relevant in the apps’ ecosystem, the study focuses on trade marks, copyright and trade secrets, which seem to be the most frequently infringed in relation to apps. However, questions about the substantive protection of these IPs in relation to apps are not explored in any great detail in the report.

#### Four main business models infringing IP

The core part of the report focuses on the four main business models applied by IP criminals when engaging in IP crime related to apps:

##### Item 2. The four business models





Within each business model, the similarities and differentiating elements in IP criminal's conduct are highlighted.

### **Infringing business model 1: infringement of copyright-protected digital content**



As copyright infringement continues to be common, copyright-protected digital content remains a priority in fighting IP-related crimes in an increasingly mobile digital environment. Both legitimate apps modified to enable copyright infringement and apps directly intended to be used for infringing purposes have been detected. Gateways enabling the download of these apps include app stores, open app stores, third party app stores, and app marketplaces. Apps can as well be installed after direct download and from various unauthorised sources. Various techniques are used as part of the criminal *modus operandi*, involving obfuscation, geo-blocking, and complex terms and conditions (T&C), among others. IP criminals have various means by which they generate revenue from these infringements, including advertising, subscription fees and revenue from commissions paid for disseminations of malware or potentially unwanted programs (PUPs). The examples of malware dissemination overlap significantly with infringing business model 3: infringement of IP for malicious and fraudulent purposes.

### **Infringing business model 2: marketing of IP-infringing physical goods**

IP-infringing physical goods are also marketed and distributed globally in the digital environment, where apps can effectively be used for such marketing purposes. The setup of this scheme differs from copyright-infringing digital content in the sense that IP criminals will necessarily have to manage the physical production, storage, distribution, and transport of the goods instead of digital storage and distribution of content. For the consumer targeted by such marketing, it is often difficult if not impossible to ascertain whether the marketed product is genuine or not. Occasionally, the marketing of IP-infringing goods will not result in actual delivery and is part of an intentionally deceptive scheme, referred to as fraudulent non-delivery. The channels through which these apps are disseminated do not differ from those mentioned in relation to infringing business model 1: infringement of copyright protected digital content. A common criminal technique in marketing through apps involves attempting to alter the app's functionalities after admission to an app store, also known as versioning. Criminal financial gains are usually derived from sales revenue, advertising, profits from non-delivery, and similar fraudulent transactions. The fraudulent examples overlap significantly with infringing business model 3: infringement of IP for malicious and fraudulent purposes.



### **Infringing business model 3: IP infringement for malicious and fraudulent purposes**



Fraudulent schemes involving IP infringement based on the use of apps are a growing threat to the safety and security of internet users and come in multiple forms. IP criminals develop, disseminate and profit from malicious and fraudulent apps by scamming, misleading, confusing and misdirecting internet users into downloading, installing and using those apps, which often imitate the trade marks of others or the appearance of legitimate apps. These apps may use cybersquatting, typosquatting, and phishing methods to attract the interest of internet users. The fraudulent apps use a multitude of techniques, including only appearing to have a certain functionality (placebo apps) whilst being packed with potentially unwanted programs (PUPs) including adware or stealth malware and other malicious programs. These apps are downloaded from the same sources as described above under business model 1: infringement of copyright protected digital content. They often bypass the requirements and security measures imposed by app stores and other app brokers. Criminal gains from these apps mainly stem from advertising, one-time download fees, fraudulent activities, and the value of intrusion and compromising devices.

### **Infringing business model 4: trade secret theft**



The theft of trade secrets by an insider or via cyber-intrusion is an especially serious IP crime related threat. This includes criminal schemes where unauthorised access and disclosure of proprietary information occur via hacking, often exploiting platform, software, or app vulnerabilities, or through social engineering. Trade secret theft can be facilitated by malicious apps used for personal or business purposes. It is occasionally directed at companies developing apps or using legitimate apps, and the misappropriation of proprietary information can be carried out by an insider as well as through cyber-intrusion. Apps facilitating trade secret theft can be downloaded from the same gateways as mentioned above under infringing business model 1: infringement of copyright protected digital content. The theft allows criminals to capture value by selling or using the stolen information. The criminal gain will usually be related to the value of the secret commercial information. The trade secret theft enabled by apps often overlap significantly with infringing business model 3: infringement of IP for malicious and fraudulent purposes.

### Nine important emerging trends

The analysis of the business models described above has aided in the identification of nine emerging threats, namely geo-blocking technologies, use of the dark web, crime-as-a-service (CaaS), superapps, versioning, use of social media and encrypted instant messaging and voice over internet protocol (VoIP) apps, digital display advertising, artificial intelligence, and payments using cryptocurrencies.

#### Item 3. Nine important emerging trends



Some of these trends are generally relevant for IP enabled by apps and many other types of IP crime (e.g., the use of dark web, crime-as-a-service (CaaS), social media, encrypted instant messaging and voice over internet protocol (VoIP) apps, artificial intelligence (AI), digital display advertising and cryptocurrencies), but some of them are especially relevant to IP crime enabled by apps (e.g., geo-blocking techniques, superapps, and versioning). When combined some of the trends becomes especially worrying, e.g., when an app using versioning and/or geo-blocking techniques is provided by an automated artificial intelligence (AI) service specialised in generating malicious or otherwise illegal code. Such services are easily and cheaply available on the dark web where most payments are done with cryptocurrencies. Such combinations of trends mean in practical terms that the entry requirements both technically and financially for engaging in highly profitable and damaging IP crime enabled by apps is relatively low and continuously is becoming lower.

### **Nine enforcement and investigative measures**

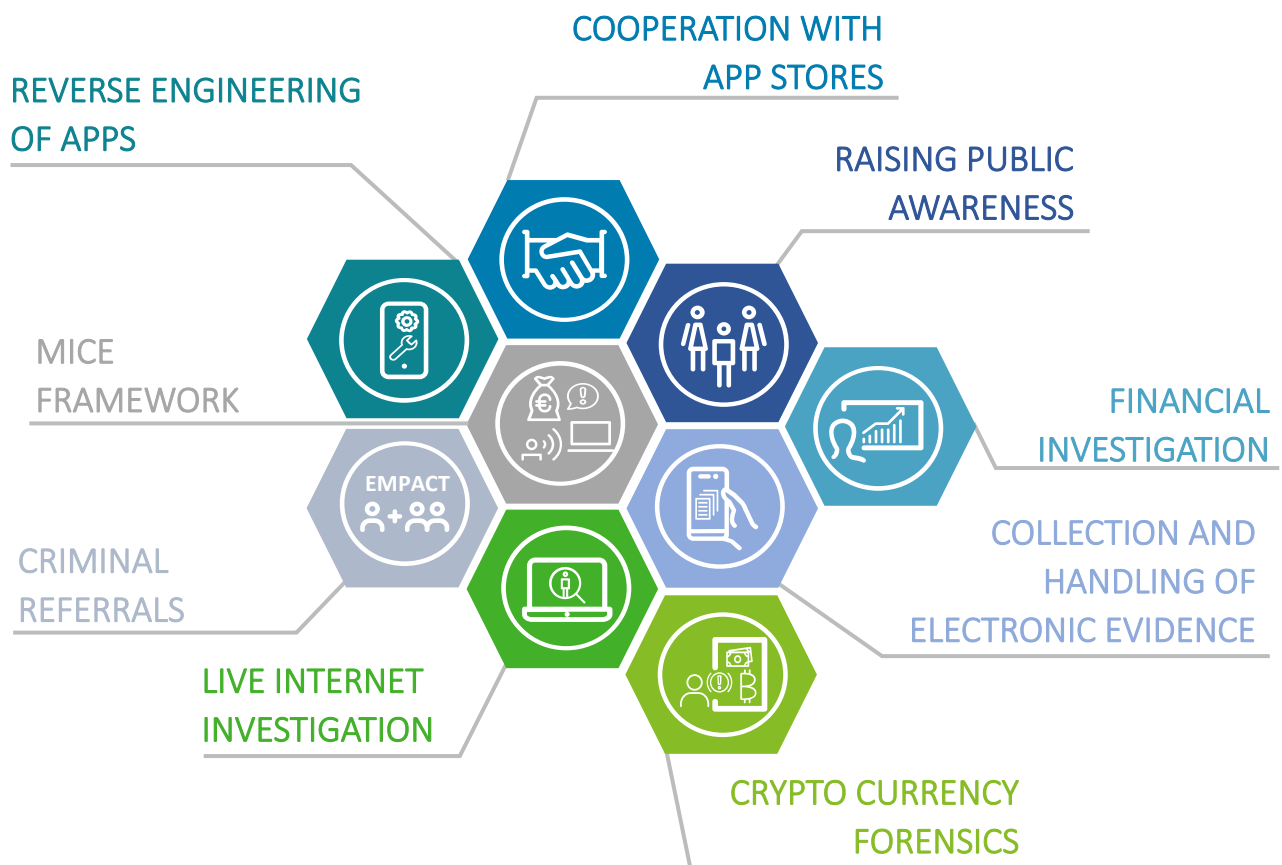
IP crime related to apps poses several enforcement challenges, depending to some extent on the specific business model used. Among the general challenges to enforcement are:

- a lack of awareness among internet users and consumers in relation to safety and security threats;
- the complex technical features and functionalities of apps;
- the need for new forensic investigative tools and methods, including those related to reverse engineering;
- a lack of required knowledge of the ecosystem among professionals working in the field of IP enforcement;
- the obfuscation techniques applied by IP criminals;
- complex jurisdictional issues;
- the need for industry, inter-agency and international cooperation, including judicial cooperation, and cooperation with intermediaries in the app ecosystem.

However, app development practices in which low-code security standards are used may make it easier to investigate the illegal practices.

To address some of these challenges, the report highlights nine enforcement and investigative measures that can be useful in the fight against IP crime related to apps, namely reverse engineering of apps, the MICE (Money-Infrastructure-Content-Exposure) framework, criminal referrals submitted to law enforcement, internet investigations, cryptocurrency forensics, financial investigation, correct collection and handling of electronic evidence; raising public awareness of the safety and security threats internet users face when downloading, installing and using fraudulent and malicious apps; and private and public sector cooperation with intermediaries in the app eco-system, including app developers and app brokers.

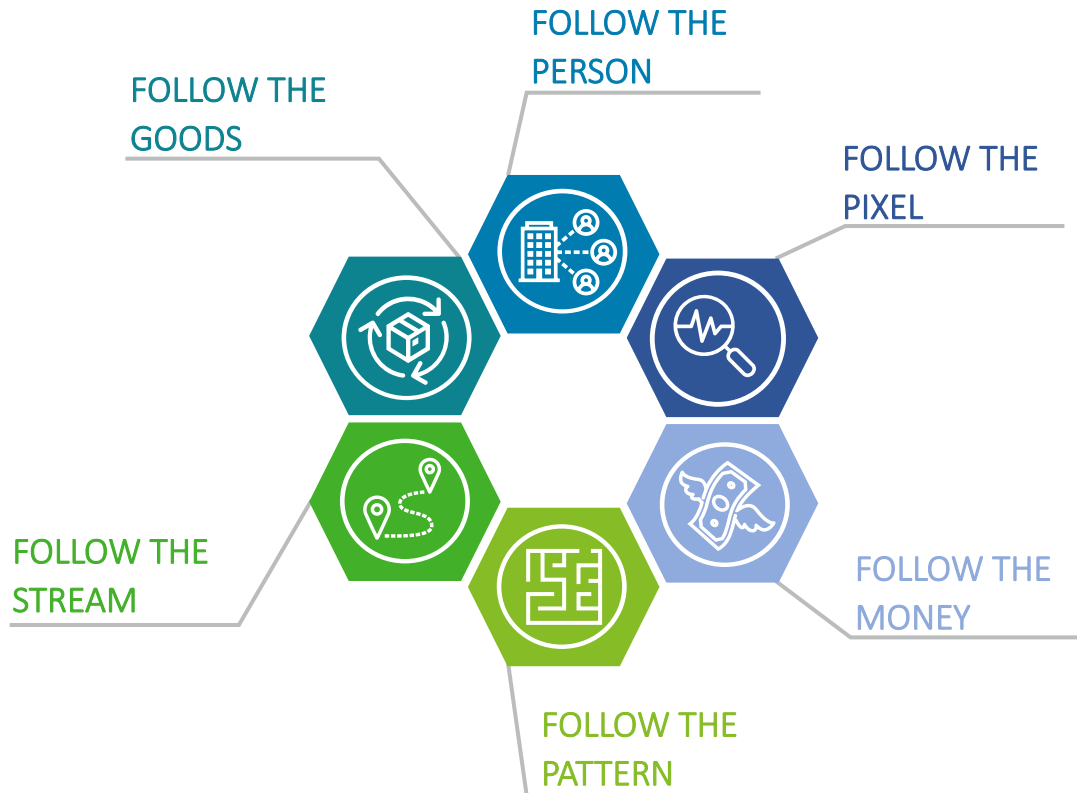
#### Item 4. Nine enforcement and investigative measures



The report also outlines specific law enforcement investigative strategies that can be effective when investigating concrete cases involving one or more of the four infringing business models analysed in the report. These strategies are traditionally named as follows:

- the *follow the goods* strategy (i.e., aiming to disclose how IP-infringing goods move through the supply chain);
- the *follow the stream* strategy (i.e., tracing the flow of copyright-infringing digital content to the source);
- the *follow the pattern* strategy (i.e., correlating individual occurrences to disclose clusters and eventually the full scope of the criminal operation);
- the *follow the money* strategy (i.e., tracing the flow of payments, advertising revenue, including cryptocurrency payments,);
- the *follow the pixel* strategy (i.e., looking for digital display advertising artefacts and related payments);
- the *follow the person* strategy (i.e., identifying the physical persons, legal persons, and any organised crime groups (OCGs) involved in the IP crime).

Item 5. **Six law enforcement investigative strategies**



At the initiation of an investigation into IP-infringement related to apps, it can be helpful to apply one or more of these specific strategies to enrich and expand the investigation. Given that each IP crime and infringing business model described herein will have varying elements, various strategies can be combined to achieve the desired result.

## Definitions

**Copyright and related rights:** a legal concept that grants the creator of an original work exclusive rights to control the use and distribution of that work for a certain period. This means that others cannot reproduce, distribute, or perform the work without the creator's permission. Copyright protection covers a wide range of creative works, including literature, music, art, and software. Closely connected to copyright is the protection of performing artists during their performances, producers of phonograms in their recordings, broadcasters in their radio and TV programmes, and other related rights.

**Copyright piracy:** commonly, copyright piracy refers to clear-cut unauthorised infringement of original creations, such as literary works, sound recordings, audiovisual works, computer software, and applied arts (e.g., original designs of customer goods and handicraft). Pirated copyright goods are copies made (a) without the consent of the IP owner(s); (b) directly or indirectly from an original article or work; and (c) where the making of that copy amounts to copyright infringement, or, in the case of imported goods, would have done so if performed within the jurisdiction.

**Counterfeiting:** although the term 'counterfeiting' is often used to refer to the unauthorised appropriation of various types of IP, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) uses it only to refer to trade mark infringements. A counterfeit mark is identical to or indistinguishable in its essential aspects from a protected trade mark. The elements in question depend on the terms of national law, but the requirements for criminal prosecution discussed in this report are these: the trade mark must be registered within the local jurisdiction; the defendant must use a counterfeit mark; the counterfeiting must be on a commercial scale; and the counterfeiting must have been committed wilfully.

**Counterfeit trade-marked goods:** Footnote 14 to Article 51 of the TRIPS Agreement states that 'counterfeit trade-marked goods' means any goods, including packaging, bearing, without authorisation, a mark that is identical to a trade mark validly registered for those goods, or that cannot be distinguished in its essential aspects from such a trade mark, and that thereby infringes the rights of the owner of the trade mark in question under the law of the country of importation <sup>(1)</sup>.

**Cyberattack:** an action that includes unauthorised access to a computer system (hacking), illegally remaining in a computer system, interference with a computer system, illegal interception of data, illegal data input, data espionage (illegal data acquisition), illegal data interference, and misuse of certain devices. The most important international legal instrument concerning cyberattacks is the Cybercrime Convention <sup>(2)</sup>. In the EU, a directive from 2013 deals with cyberattacks <sup>(3)</sup>.

---

<sup>1</sup> [Trade-Related Aspects of Intellectual Property Rights \(TRIPS Agreement\)](#)

<sup>2</sup> [Cybercrime Convention](#)

<sup>3</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040>

**Cyberfraud and cyberforgery:** a type of criminal act committed online using electronic communications networks and information systems to commit online fraud or forgery. Large-scale fraud can be committed online using techniques such as cybersquatting, typosquatting, identity theft, phishing, spam, and malicious code. The most important international legal instrument concerning cyberfraud and cyberforgery is the Cybercrime Convention <sup>(4)</sup>. In the EU, a directive from 2019 deals with combating fraud and counterfeiting of non-cash means of payment <sup>(5)</sup>.

**Cybersquatting:** a term usually used to describe the unauthorised registration and use of a domain name that is identical or similar to another's trade mark (see also typosquatting).

**Design:** the appearance of the whole or a part of a product (any industrial or handicraft item, including inter alia parts intended to be assembled into a complex product, packaging, get-up, graphic symbols and typographic typefaces, but excluding computer programs) resulting from the features of, in particular, the lines, contours, colours, shape, texture and/or materials of the product itself and/or its ornamentation <sup>(6)</sup>.

**EMPACT:** European Multi-disciplinary Platform against Criminal Threats. EMPACT is a security initiative driven by EU Member States to identify, prioritise and address threats posed by organised and serious international crime <sup>(7)</sup>.

**Infringement of intellectual property (IP):** a term that directly covers IP-infringing acts as well as (for the purposes of this report) contributory and preparatory acts in furtherance of conspiracies and attempts to commit IP infringement and other closely related illegal acts or criminal offences (e.g., cybercrime offences and money laundering).

**Intellectual property (IP):** creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce to identify the origin of goods and services, plant varieties, geographical indications, and commercial secrets. IP is protected in various international legal instruments and national laws. For the purposes of this study, the most important IPs are copyright, trade marks, and trade secrets.

**Intellectual property (IP) crime:** IP crime depends on national legislation. The only international (or EU standards) concerning IP crime are the provisions in Article 61 of the TRIPS Agreement <sup>(8)</sup> concerning wilful trade mark counterfeiting or copyright piracy on a commercial scale, and Article 10 of the Cybercrime Convention <sup>(9)</sup> concerning crimes related to infringements of copyright and related rights.

**Organised crime group (OCG):** a group of three or more persons existing over a given period and acting in concert with the aim of committing crimes for financial or material benefit, according to the definition adopted in the United Nations Convention against Transnational Organised Crime (2000) <sup>(10)</sup>. This definition does not preclude investigations of two or more

---

<sup>4</sup> [Cybercrime Convention](#)

<sup>5</sup> [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2019.123.01.0018.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG)

<sup>6</sup> [EU community designs legal text](#)

<sup>7</sup> <https://www.europol.europa.eu/crime-areas-and-statistics/empact>

<sup>8</sup> [Agreement on Trade-Related Aspects of Intellectual Property Rights \(TRIPS Agreement\)](#)

<sup>9</sup> [Cybercrime Convention](#)

<sup>10</sup> [United Nations Convention against Transnational Organised Crime](#)



persons for conspiracy to commit an IP crime. This definition was also adopted in the EU's Council Framework Decision 2008/841/JHA of 24 October 2008 in the fight against organised crime <sup>(11)</sup>.

**Patent:** an invention, in any field of technology, provided that it is new, involve an inventive step and is susceptible of industrial application <sup>(12)</sup>.

**Pirated copyrighted works:** Footnote 14 to Article 51 of the TRIPS Agreement <sup>(13)</sup> states; 'pirated copyright goods shall mean any goods which are copies made without the consent of the IP owner or person duly authorised by the IP owner in the country of production and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under the law of the country of importation'. Although the definition in the TRIPS Agreement refers to 'goods', it applies equally to the piracy of online copyrighted works.

**Trade mark:** a sign, in particular words, including personal names, or designs, letters, numerals, colours, the shape of goods or of the packaging of goods, or sounds, or a combination of these elements, provided that such signs are capable of distinguishing the goods and services of one undertaking from those of other undertakings <sup>(14)</sup>. A trade mark serves to identify and distinguish the goods or services of a particular company or individual from those of others in the marketplace. Trade marks help customers easily recognise goods or services with a particular brand or source. In addition, trade marks are usually registered with the state to provide legal protection against unauthorised use by others and are important for businesses because they help build brand recognition and reputation.

**Trade secrets:** According to European Union Directive 2016/943 <sup>(15)</sup>, a trade secret is information that meets all of the following requirements:

- it is secret, in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- it has commercial value because it is secret;
- it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

**Typosquatting:** a term usually used to describe the unauthorised registration and use of a domain name that is similar to another's trade mark (see also cybersquatting).

---

<sup>11</sup> [Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime](#)

<sup>12</sup> [European Patent Convention](#)

<sup>13</sup> [Agreement on Trade-Related Aspects of Intellectual Property Rights \(TRIPS Agreement\)](#)

<sup>14</sup> [EU trade mark legal texts](#)

<sup>15</sup> [Directive \(EU\) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information \(trade secrets\) against their unlawful acquisition, use and disclosure](#)

## I Background, scope, and methodology

### I.A Background

In terms of technology, one of the major effects of globalisation and the proliferation of internet-connected devices has been the development of applications (apps) – especially those on mobile electronic devices, televisions, gaming devices and other Internet of Things (IoT) devices<sup>(16)</sup>. The functionalities of apps have quickly expanded beyond basic operations such as managing contact lists, browsing, email, and calendar functions, and have now expanded into other areas of online activities, including e-commerce, banking, public services, gaming, entertainment, culture, sports, health and wellness, and education. Therefore, an increasingly important way of attracting users is through the creation and dissemination of an app.

Given this growth, app creation is becoming an increasingly important way of attracting users. Paying attention to apps and the app ecosystem has become a significant part of efforts to protect and enforce intellectual property (IP), including promotion of the IP, brand protection strategies, and the investigative and prosecutorial efforts of law enforcement and judicial authorities. As IP protection and enforcement practices develop – whether related to the marketing of physical goods protected by one or more IP, the dissemination of copyright-protected digital content, the use of digital identifiers and fraud related to trade marks, or trade secrets – apps are being given increasingly serious consideration.

The various types of apps<sup>(17)</sup>, for different devices, can all be misused by IP criminals to host, promote, distribute, reproduce, or offer IP-protected content, services, or products to users. At a high level, apps can be divided into five categories: consumer service apps, media apps, social media apps, communication apps and utility apps. Just as websites, domain names, and online platforms are the venues for commercial activities and can be used to commit illegal acts like fraud, cyberattacks, and the dissemination of malware and IP infringements, these categories of apps can also be misused in this way. As such, the focus on apps is on those that are either in themselves IP-infringing (e.g., infringe a trade mark), or are specifically designed to infringe or facilitate infringement (e.g., some branded IPTV apps), or do not initially infringe IP but by way of functionality, configuration or modification can be used for such purposes (e.g., some generic media players).

IP-infringement facilitated by apps can often be related to other elements of criminal activity making it a priority to effectively combat IP infringement and, resultingly, lessen the threats posed to internet users, infrastructure providers, and IP owners and their organisations while reducing the potential support for more extensive illegal activities.

---

<sup>16</sup> Internet-connected devices are all those that function together, or independently, through a connection to the internet of things (IoT). IoT technologies span from traditional computing, to smartphones, tablets, gaming devices, cameras, television sets, GPS devices, or drones.

<sup>17</sup> Outside the scope of this study are desktop apps for computers, and apps related to legal content-sharing services, social media services (including messaging services), and other traditional digital services, unless an application offers specific functionalities or features that allow misuse of legal services to infringe IP.

Therefore, two joint papers from EUROPOL and EUIPO <sup>(18)</sup>, and the EUIPO ‘Study on Business Models Infringing Intellectual Property – Phase 5: Modus Operandi of Serious and Organised Crime’, provide information on organised crime groups (OCG) committing IP crime <sup>(19)</sup>. The final conclusion is that IP crime is often interlinked with other types of illegal activities, either as a supporting or as a parallel activity. The studies show how a variety of crimes, including money laundering, document fraud, cybercrime, fraud, narcotics crime, and human trafficking are connected to IP crime, effectively reaffirming that IP crime is not a victimless crime. Understanding the connections between IP crime and other criminal activities can aid policymakers, law enforcement officials, prosecutors, IP owners and others with an interest in IP protection and enforcement in addressing IP crime on both a policy and enforcement level.

In 2021, the European Union’s Council of Ministers included IP crime among the top priorities in the fight against organised crime for 2022-2025. These will be addressed through the European Multi-disciplinary Platform against Criminal Threats (EMPACT), a security initiative driven by EU Member States to identify, prioritise and address threats posed by organised and serious international crime. EMPACT Priority 7 targets fraud, economic and financial crimes. In its Aim 4, which is specifically related to IP crime and counterfeiting of goods and currencies, it proposes, inter alia, ‘to combat and disrupt criminal networks and criminal individual entrepreneurs involved in IP crime and in the production, sale or distribution (physical and online) of counterfeit goods or currencies, with a specific focus on goods harmful to customers’ health and safety, to the environment and to the EU economy’ <sup>(20)</sup>.

In March 2024, the Commission adopted a comprehensive set of recommendations to enhance the fight against counterfeiting and improve protection of IP <sup>(21)</sup>. The recommendations included a number of key actions aimed at providing a robust criminal enforcement regime concerning serious and organised IP crime.



*The people running criminal networks are career criminals and have found that it is easy, carries low risk, and is very profitable. What society has to do is make it so painful, awkward, troubling and difficult for them that they move away from crime.*

IP crime expert

<sup>18</sup> EUIPO / Europol (2019), ‘[Intellectual Property Crime Threat Assessment 2019](#)’, and EUIPO-Europol (2020), ‘[IP crime and its link to other serious crimes. Focus on Poly-Criminality, June 2020](#)’.

<sup>19</sup> EUIPO ‘[Study on Business Models Infringing Intellectual Property – Phase 5: Modus Operandi of Serious and Organised Crime](#)’.

<sup>20</sup> Read more about the EMPACT framework here: <https://www.europol.europa.eu/crime-areas-and-statistics/empact>.

<sup>21</sup> Read more here: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_24\\_1551](https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1551)

## I.B Scope

The research study series on business models infringing IP has been an activity of the European Union Intellectual Property Office (EUIPO), through the European Observatory on Infringement of Intellectual Property Rights ('the Observatory'), since 2016.

The initiative was launched to develop independent expert information based and data-driven studies that would assess and analyse how commercial-scale online IP infringements work, including how they are financed and generate profits for their operators, as well as what kind of content is disseminated, what kind of products are marketed, and how large the user bases are.

The results of the studies provide policymakers, civil society, academia, private businesses, law enforcement authorities and the judiciary with an enhanced understanding of the IP infringement landscape. At the same time, it can help identify and better understand the range of responses required to tackle the challenges of large-scale IP infringements.

Since 2016, the EUIPO has published five reports on business models infringing IP:

- In 2016, the EUIPO published a report entitled [Establishing an overview of online business models infringing intellectual property rights](#). The initiative was an independent data-driven study that aimed to provide an overview of various IP-infringing business models by assessing how they function, how they are financed, how they generate profits for their operators, what content they disseminate, and how large their user bases are.
- In 2017, the EUIPO published a study focused on [Suspected trade mark-infringing e-shops utilising previously used domain names](#). Phase 1 of the report was published in July 2016 and focused on online IP-infringing business models. For its Phase 2, the study focused on the misuse of deleted domain names to market IP-infringing goods in Germany, Spain, Sweden, and the UK. This phase emphasised the need for broad cooperation among authorities to combat these abuses. The research involved an in-depth analysis of country code top-level domains (ccTLD) to identify e-shops suspected of marketing trade mark-infringing products.
- In 2019, the EUIPO issued a study on [Illegal IPTV in the European Union](#) aimed at enhancing understanding of the methods of broadcasting illegal internet protocol television (IPTV) and how the associated business models function. This was in order to provide a basis for subsequent identification of possible responses to tackle the crime more effectively.
- In 2020, the EUIPO initiated a research study on IP infringement through [Vendor Accounts on Third-Party Trading Platforms](#). The purpose of the research was to better understand the criminal misuse of online trading platforms to market goods and services that infringe IP, and to examine the business models adopted by IP criminals to provide new knowledge that could be used in enforcing IP more effectively.

- Lastly, in 2023, the EUIPO published a report on the [Modus Operandi of Serious and Organised Crime](#), exposing how serious and organised crime groups generate profits by infringing IP in various sectors such as textiles, footwear, toys, and sports equipment. It also highlighted the importance of law enforcement agencies, IP owners, and e-commerce platforms working together on enforcement.

Following the methodology and approach of the first five phases, the scope of the current Phase 6 aims to achieve the following:

- to identify and analyse specific business models – in this case, based on or involving apps – that are used to facilitate IP infringements on a commercial scale;
- to identify the drivers and enablers behind the use of these apps;
- to elaborate on the use of these apps within serious and organised crime;
- to analyse the IP crime landscape and identify the potential challenges ahead, focusing on the infringing and often criminal use of online apps.

It is outside the scope of this research study to determine whether an online activity in fact infringes one or more IP since such a determination can only be made in a judicial procedure. For these purposes, terms like ‘suspected IP-infringing’ are used unless the example has been through a court proceeding. As such, the examples of services included within this report have been vigilantly anonymised to remain within the scope of this research study (as explained within I.C on methodology). Ultimately, this report intends to provide a snapshot of the situation as detected by practitioner’s and shared in interviews.

## I.C Methodology

### *I.C.1 Research deliverables*

The development of the study was entrusted to Deloitte Advisory, S.L., specifically the group focused on Fraud Prevention and Financial Crime matters and supported by the Observatory network.

The methodological approach for this study on apps enabling IP crime, encompasses two main, clearly distinct yet complementary, parts.

Accordingly, the project team collected material on suspected app enabled business models by following the methodology of the previous research series and mainly collecting information through structured interviews with experts in the field, as well as case-law from national courts. The project also considered practical examples referred to in various reports by public authorities, international organisations, or other reliable and publicly available sources.

As emphasised above, the examples used within this report have been anonymised as much as possible. Additionally, examples where a court of law has not determined that an IP infringement has occurred will be considered merely to be suspected of IP infringement, following the policy that only a court of law may finally determine whether an activity infringes IP or not.

This study report is the first deliverable of the research project and is based on:

- a literature review of existing studies and reports on the topic;
- an examination and analysis of the most relevant jurisprudence (covering Australia, China, Denmark, France, Germany, India, Italy, Spain, the United Kingdom, and the United States);
- two hands-on workshops conducted in early 2023 with members of the Observatory Impact of Technology expert group, as well as public and private sector experts identified and recruited from the Observatory network;
- a series of semi-structured interviews (28 in total) with experts representing numerous sectors<sup>(22)</sup> that considered the views of anti-piracy associations, and expert experience on cybersquatting, typosquatting, and IP-infringing goods, brand protection, counterfeits, piracy, technology, apps ecosystems, judiciary, and law enforcement;
- independent research focusing on the marketing, sharing, use and commercialisation of apps, including use of proprietary software solutions<sup>(23)</sup>.

The report will be followed by a collection of investigative practices and training materials specifically aimed at and made available for law enforcement and the judiciary.

The content of this report is complementary to the research led by the Observatory through the Cooperation with Intermediaries Expert Group on the misuse of Apps and App stores, focusing on how this ecosystem can be misused for intellectual property infringing activities, and how these misuses can be counteracted through good practices. A discussion paper on the topic will be published in parallel with this report (see III.B.1).

## *I.C.2 The arc of IP crime related to apps*

While most types of IP are relevant to the app ecosystem, this study focuses mainly on infringements of trade marks and copyright, and theft of trade secrets. However, questions about the substantive protection of these rights in regard to apps are not explored in any great

---

<sup>22</sup> Sectors included music, sports, audiovisual, television, IPTV, consumer goods, and gaming.

<sup>23</sup> Deloitte's FakeFinder service draws on information and characteristics of the original products to establish the basis for information gathering and detection of findings. The tool uses anti-counterfeiting AI technology with the application of machine learning and AI techniques to determine the legitimacy of the products found. This process leads to a subsequent analysis, carried out by a specialised team.

detail in the report. The main focus is on how infringements of the three IPs in focus can be enabled by the misuse of apps.

The core part of the report describes the four main business models applied by IP criminals when engaging in IP crime related to apps:

#### Item 6. The four business models



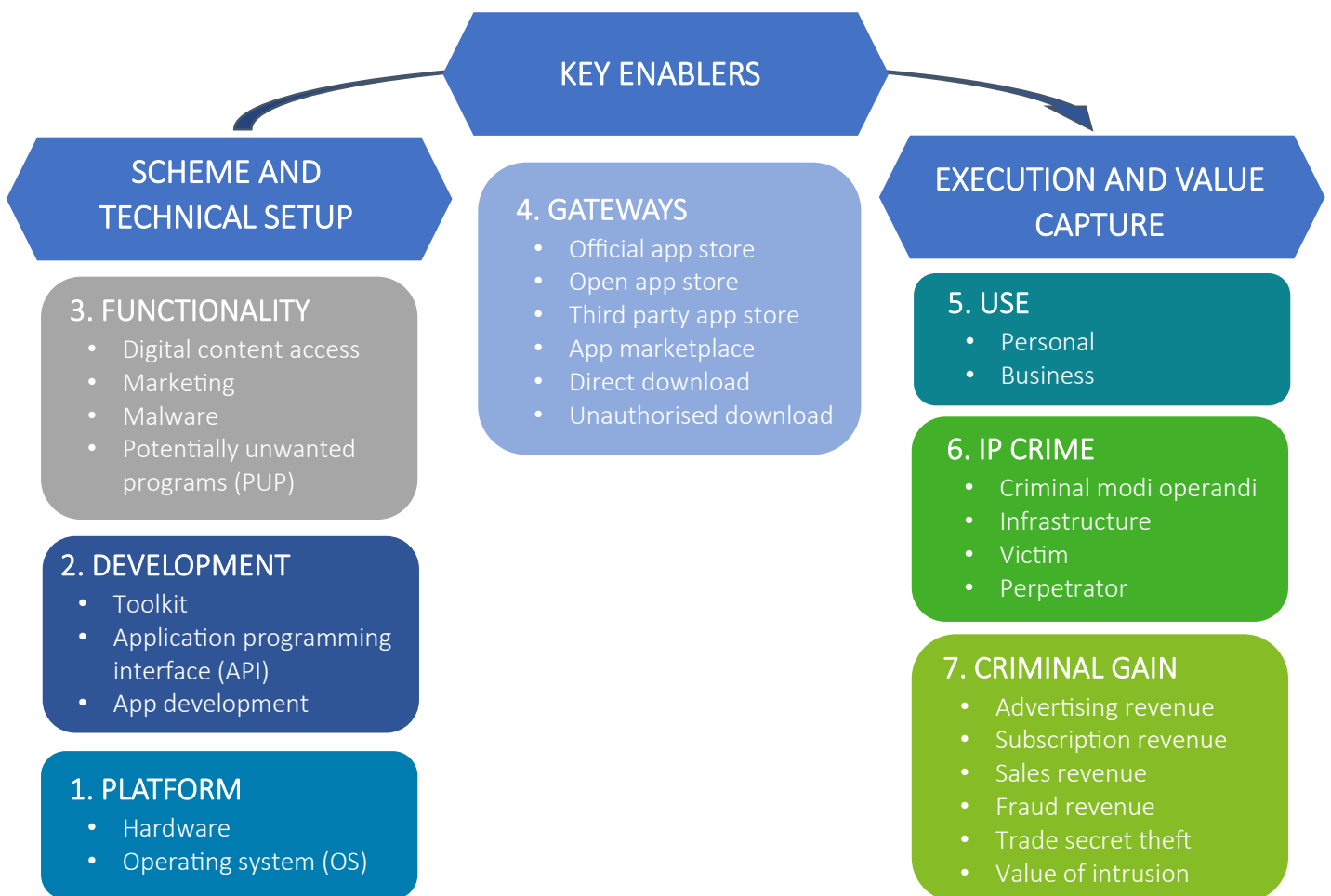
A unique graphical model named *the arc of IP crime related to apps* was created to depict the seven elements of app-related IP crime and provide an organised analysis of the business models examined. This graphical model was inspired by existing descriptions of the app ecosystem <sup>(24)</sup> and focuses on three main elements, divided into seven separate parts:

- The scheme and technical setup:
  - platform: technical environment in and for which an app is developed;
  - development: the methods that the app developers use to create the app;
  - functionality: the ultimate intended features of the application.
- The key enablers: gateways: the channel or channels on which the app is made available to users.

<sup>24</sup> E.g., Ioannis Iglezakis, et. All (2020), 'Legal Issues of Mobile Apps: A Practical Guide'.

- The value capture and gain achieved by IP criminals:
  - Use: the practical use for the app’s target audience;
  - IP crime: the specific criminal elements in each of the four IP-infringing business models identified in this report;
  - criminal gain: the monetary or non-monetary advantage obtained by IP criminals.

Item 7. *The arc of IP crime related to apps*





### *I.C.3 Analysis of collected data*

Based on the data collection and the arc of IP crime related to apps graphical model, the relevant information for the report was analysed and compiled, and training materials were prepared. The number and types of relevant apps available, and their means of delivery, were specified. Technical analyses of the types of apps used for IP-infringing activities were carried out, together with an analysis of the various app ecosystems.

This part of the research study included the following.

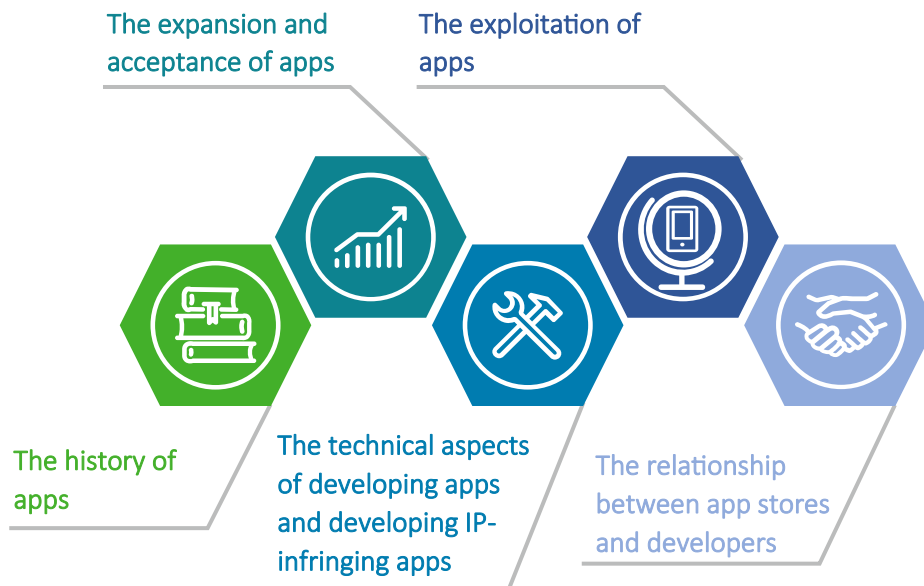
- Several relevant and available apps and their means of delivery were subjected to a technical analysis, in which the various apps were categorised and rated according to their relevance. The documentary study was considered in this section to understand the types of existing apps based on their technical characteristics, categorise the apps according to the content offered to users, and provide a general overview of the main apps infringing IP.
- The technical analyses of the types of apps used for IP-infringing activities covered two main scenarios: (1) apps that infringe IP themselves; and (2) apps whose functionality and configuration enables IP criminals to commit such crimes, given a lack of enforcement. The analysis made use of technical tools used to prevent IP crimes.
- A mixed-method analysis of how serious and organised crime is conducted through apps, focusing on the ways that IP crimes are committed. Empirical and qualitative techniques were used to assess how these criminal activities are conducted, and an in-depth analysis was carried out to understand the possible existence of illicit ecosystems behind such apps – focusing not only on the surface web but also the dark web (see III.A.2).

### *I.C.4 Structure of the report*

The first substantive chapter in the final report (see II) consists of a description of the app ecosystem, including:

- the history of apps;
- the expansion and acceptance of apps;
- the technical aspects of app (and particularly IP-infringing app) development;
- the exploitation of apps;
- the relationship between app stores and other app brokers.

Item 8. The structure of the first chapter of the report



The main part of the report analyses and describes the four main types of IP-infringing business model. Each of these chapters is meant to be self-contained, and a certain degree of overlap and repetition has therefore been unavoidable. Consequently, relevant cross-references are used throughout to link the sections.

Information on each business model will be accompanied by a representative graphic; the four business models are as follows:



- Infringing Business Model 1: infringement of copyright-protected content (see III).

- Infringing Business Model 2: marketing of IP-infringing physical goods through apps (see IV).



- Infringing Business Model 3: IP infringement for malicious and fraudulent purposes (see V).

- Infringing Business Model 4: trade secret theft (see VI).



For a cohesive analysis of the distinctive infringing business models, the basis for the analysis will be the unique *arc of IP crime related to apps* developed specifically for this study. The backbone of the graphic contains three main elements: the scheme and technical setup; the key enablers; and the value capture and gain. Moreover, this report will consider apps downloaded from any app gateway, including, inter alia, well-known app stores, open app stores, app marketplaces, as well as through any other sources.

The analysis constitutes a simplified and structured elucidation of the subject matter, emphasising overarching concepts rather than delving into exhaustive technical intricacies of applications. This report's primary objective is to underscore significant facets of the application ecosystem as they pertain to IP crime. The information gathered by the provider of the study – predominantly consisting of practitioner interviews – is not intended to be exhaustive in terms of concepts, examples, technical descriptions and detail, and, due to nature of the subject matter, some aspects might overlap in different sections of the report, reflecting the interconnected nature of the topics discussed.

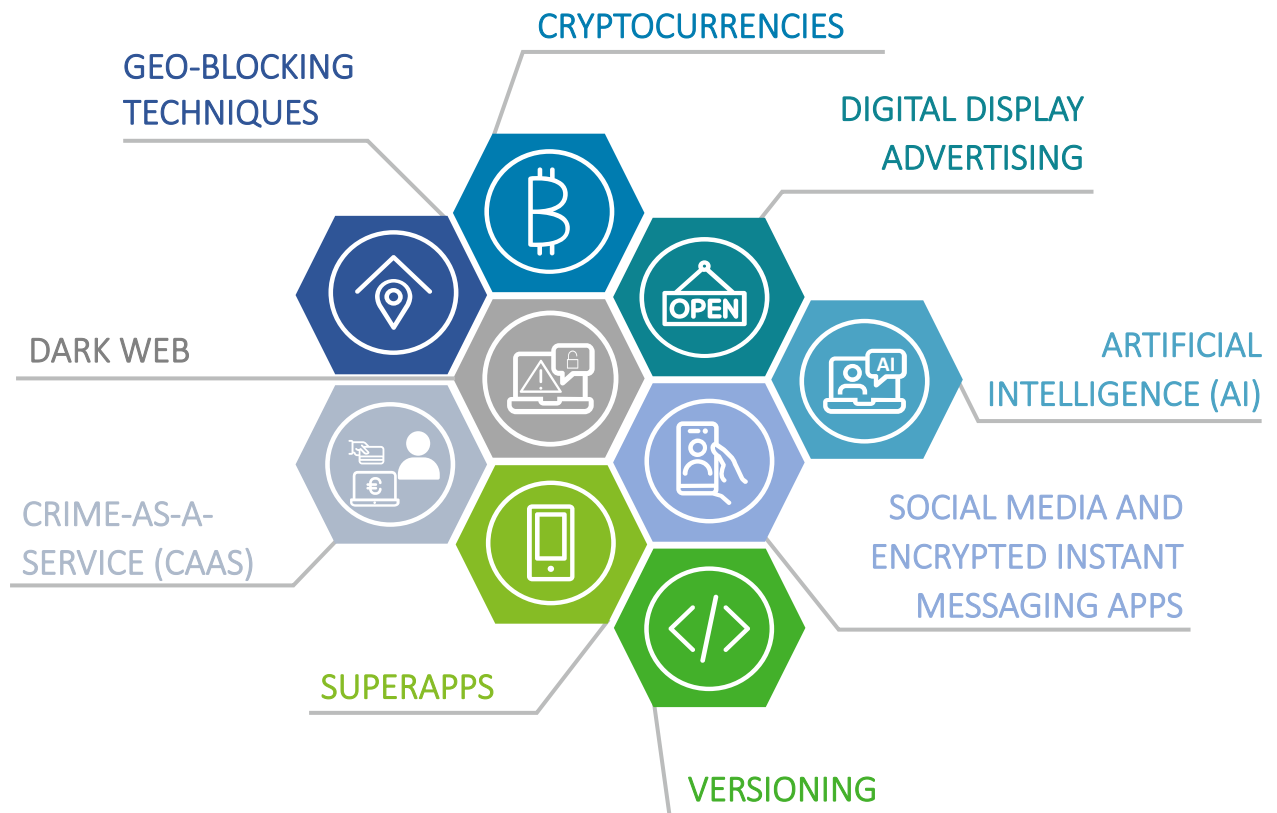
Throughout the chapters of the report, the following case examples are integrated to further the analysis of the infringing business model related to apps:

## Item 9. Overview of case examples

Case example	Description
<b>App piracy group</b>	In a landmark action, the US Department of Justice, with Dutch and French law enforcement, seized domains like <i>applanet.net</i> , <i>appbucket.net</i> , and <i>snappzmarket.com</i> due to their illegal distribution of infringing copies of copyrighted Android apps. This marked a major effort against digital copyright infringement, resulting in the conviction of nine individuals in three different online organised crime groups which, together, distributed millions of pirated apps, valued at over \$19 million. The case highlighted the international commitment to enforcing IP rights and combating digital piracy (See III.A.1).
<b>Modbro</b>	The Mobdro app case spotlighted the legal repercussions of streaming copyrighted content without authorisation via IPTV technology. Facilitating access to TV shows, movies, and sports without proper permissions, Mobdro attracted lawsuits from copyright holders and law enforcement actions across various jurisdictions. This legal battle emphasised the growing efforts to enforce intellectual property rights within the app ecosystem and highlighted the risks for creators and users of unlicensed streaming services in facing significant legal challenges (see III.C.3.d).
<b>Popcorn time application</b>	Popcorn Time, a P2P based network enabling users to stream copyrighted content without permission, faced significant legal challenges globally. Declared illegal by the US District Court of Oregon in 2015 and by the Danish Supreme Court in 2020, the platform was criticised for facilitating IP infringements. Despite efforts to block access in countries like the UK, the anonymity of its creators and the proliferation of variants have complicated copyright enforcement, underscoring the ongoing battle against digital piracy (see III.C.3.c).
<b>Waymo v. Uber</b>	In a high-profile legal battle, Waymo accused Uber of conspiring with a former engineer to steal trade secrets related to driverless vehicle technology. The dispute centred on the alleged misappropriation of 14 000 files, crucial to Waymo's lidar technology, essential for autonomous vehicles. Waymo sought USD 1.8 billion in damages, but ultimately settled for approximately USD 244 million in Uber equity and assurances against the use of its trade secrets, underscoring the importance of intellectual property protection in the tech industry (see VI.C.2.a).
<b>Xtream codes</b>	The Xtream Codes case involved a significant legal battle over a software platform used by IPTV providers to stream copyrighted content without authorisation. In September 2019, a joint operation by Italy, France, and Bulgaria led to the shutdown of Xtream Codes and the detention of its operators, highlighting efforts to combat digital copyright infringement. However, in a twist, the Court of Appeals of Naples ruled in August 2021 that there was no evidence Xtream Codes Ltd had acted illegally, underlining the complexities of copyright law in the digital era (see III.A.3).

Apps also give rise to several emerging threats, nine of which are integrated into the report.

Item 10. **Nine important emerging trends**



A text box for each of the emerging threats can be found at the following locations:

- Geo-blocking: see V.A.3.c;
- Dark web: see III.A.2;
- Crime-as-a-service (CaaS): see III.A.2.a;
- Superapps: see IV.C.2.c;
- Versioning: see IV.A.3;
- Social media and encrypted instant messaging and voice over internet protocol (VoIP) apps: see III.C.3.d;
- Artificial intelligence (AI): see II.D.2;
- Digital display advertising: see III.C.3.a;
- Cryptocurrencies: see V.C.3.

Criminal investigations carried out by law enforcement authorities are increasingly important in the field of IP crime <sup>(25)</sup>; while a comprehensive description of criminal investigation falls outside the scope of this report, six investigative strategies that can be applied in IP crime cases related to apps are outlined for each of the business models:



The **follow the goods** strategy extends beyond the mere prevention or disruption of the marketing or sale of IP-infringing goods. The focus is on investigating the supply chain from the retail to the wholesale level to identify importers and distributors. In some cases, the investigation may even extend to the manufacturing level to identify the financers and manufacturers, especially in cases of domestic or regional production. See use of the strategy in III.C.3.e and IV.C.2.d.

The **follow the stream** strategy identifies the actual content from the consumer up to its source. It can be difficult to map the full stream, detailing each particular criminal network from end to end – especially given IP criminals' use of state-of-the-art anonymisation technologies. However, investigators can carefully compile various clues and indicators using this strategy. See use of the strategy in III.C.3.e and IV.C.2.d.



The **follow the pattern** strategy entails investigative techniques geared towards finding connections and correlations between websites, posting on e-commerce platforms, the dark web, social media, and encrypted messaging app accounts, as well as any other online activity, even if they appear unrelated. The particular techniques may include internet investigations (e.g., open-source intelligence (OSINT), and obtaining data, information, intelligence, and/or evidence from online intermediaries, among others). See use of the strategy in III.C.3.e, IV.C.2.d, V.C.2.f, VI.C.2.a and VI.C.2.b.

The **follow the money** strategy deals with payment flows and is the most crucial and effective strategy in enriching an investigation. This strategy can be used within each of the four infringing business models, as financial gain is the dominant motive in most IP criminal activity. Even in cases where there is no financial motive, there will nevertheless probably be a money trail related to the physical and digital infrastructure used by the IP criminal. See use of the strategy in III.C.3.e, IV.C.2.d, V.C.2.f, VI.C.2.a and VI.C.2.b.



The **follow the pixel** strategy describes investigations into all online advertising related technologies, as they are an integral part of apps. The investigative thread can be easily found given the requirement for beneficiaries to be identified when receiving advertising revenue. This strategy becomes very effective when combined with the 'follow the money' strategy. See use of the strategy in III.C.3.e.

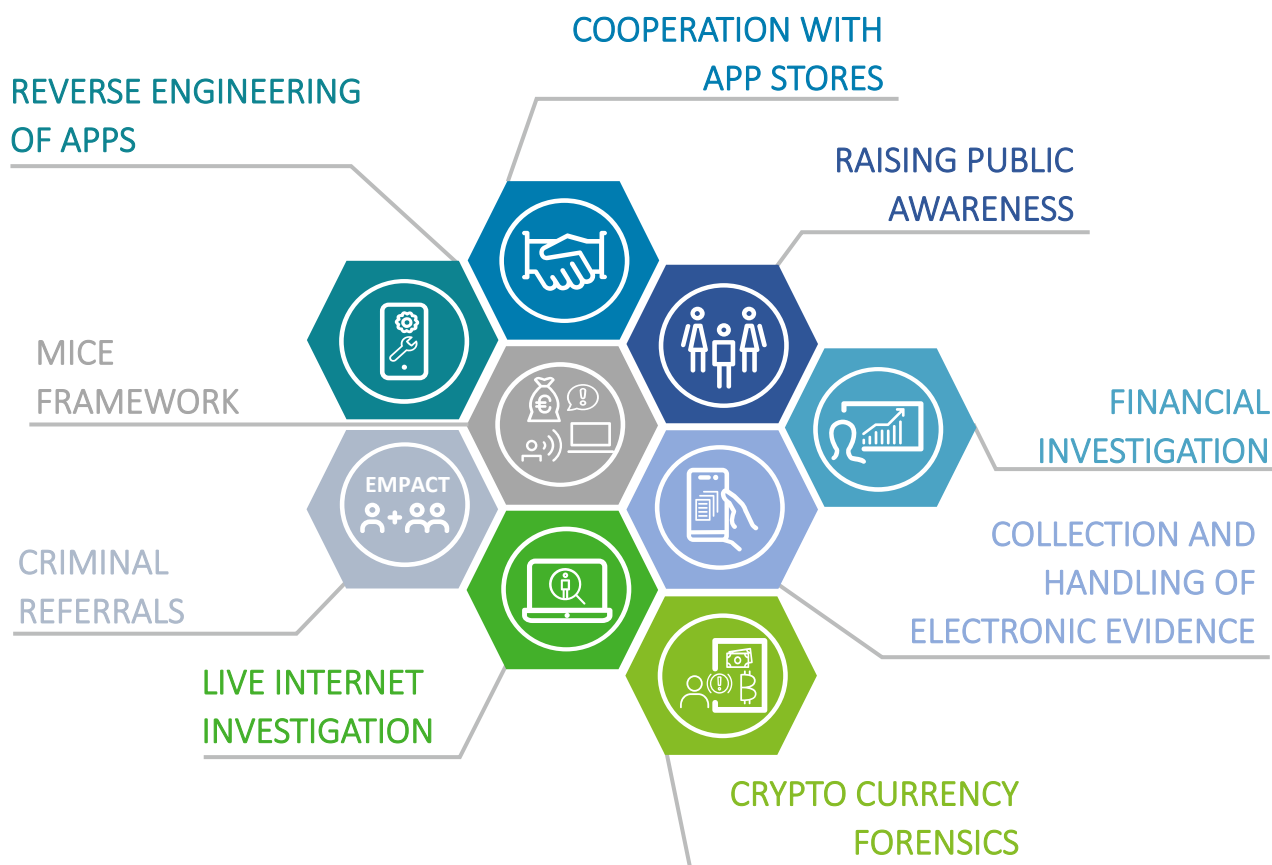
<sup>25</sup> See footnote 20.

The **follow the person** strategy describes investigative approaches aimed at identifying the physical persons involved in an IP crime, their affiliations, and their cooperation structure. This includes the identification of any limited-liability companies used by IP criminals to launder generated revenue. Specific techniques may include internet investigations, financial investigations, or covert investigations. See use of the strategy in IV.C.2.d and VI.C.2.a.



To achieve the goals expressed by the investigation strategies, nine enforcement and investigative measures have been highlighted. These measures are not only relevant to public investigative authorities but also, to some extent, to private sector entities involved in IP enforcement and investigation.

Item 11. **Nine enforcement and investigative measures**



A text box for each of the enforcement and investigative measures can be found at the following locations:

- Reverse engineering: see III.A.2.c;
- MICE Framework: see III.C.2;
- Criminal referrals: see II.E.1.b;
- Internet investigation: see V.C.2.b;
- Cryptocurrency forensics: see III.C.3.b;
- Collection and handling of electronic evidence: see VI.A.1;
- Financial investigation: IV.C.3;
- Raising public awareness: see V.C.1;
- Cooperation with app developers and app stores: see III.B.1.

The final chapter (see VII) contains some conclusions on the findings of the report and provides tables with overview of:

- Techniques use for criminal purposes: see VII;
- Revenue sources: see VII;
- Enforcement and investigative approaches: see VII.



## II App ecosystem

### II.A History of apps

As mobile phones become more popular, and more sophisticated features are made possible by technical breakthroughs, it is worth recalling that the history of mobile apps, particularly those apps that fall within the scope of this study, go back to the mid-1990s and early 2000s. The first smartphone that contained apps was IBM's Simon, which offered 10 built-in apps including a calculator, an address book, a mail app, a notepad, and a sketchpad<sup>(26)</sup>. Initially, apps were straightforward and confined to pre-installed tools, including games like Snake<sup>(27)</sup>. Apps native to other platforms, like television sets and gaming platforms, have also undergone advancements as the technologies developed.

However, with the release of smartphones like the iPhone in 2007 and Android handsets in 2008, the mobile industry underwent a major change, giving programmers a platform to create and distribute external apps. The introduction of Apple's App Store in 2007 offered smartphone customers a centralised marketplace to find, download, and update mobile software.

As iOS and Android grow increasingly sophisticated and contextually aware, they are giving developers the tools they need to gather and respond to these signals, while delivering them quickly and thoughtfully to users<sup>(28)</sup>. Apps are so widely available now that anyone may create them, either independently or by involving a third-party. The Google Play Store had 3.48 million apps available in the first quarter of 2021, while the iOS app store had 2.22 million. Apps are as useful to creators as they are to users when the ease of creation is combined with a possible return on investment, either in terms of utility or cash<sup>(29)</sup>. The integration of apps extends beyond smartphones and forms part of other technologies, such as smart televisions and gaming consoles, contributes to their growing complexity.

*Typically, when dealing with mobile apps, there are different scenarios. 10 years ago, there were only native apps developed for specific platforms. Now, cross-platform apps have entered the market at scale.*

IP crime expert

A detailed timeline outlining the most important event shaping this industry has been developed to help understand the extraordinary journey of mobile apps. Beginning with mobile apps, which were the groundbreaking innovation that led to apps being contained in other devices, the following graphic illustrates the way in which developments have snowballed and led to the 'app store revolution'.

<sup>26</sup> Doug Pittman (2020), [A Brief History of Mobile Apps](#), accessed on 15 May 2023.

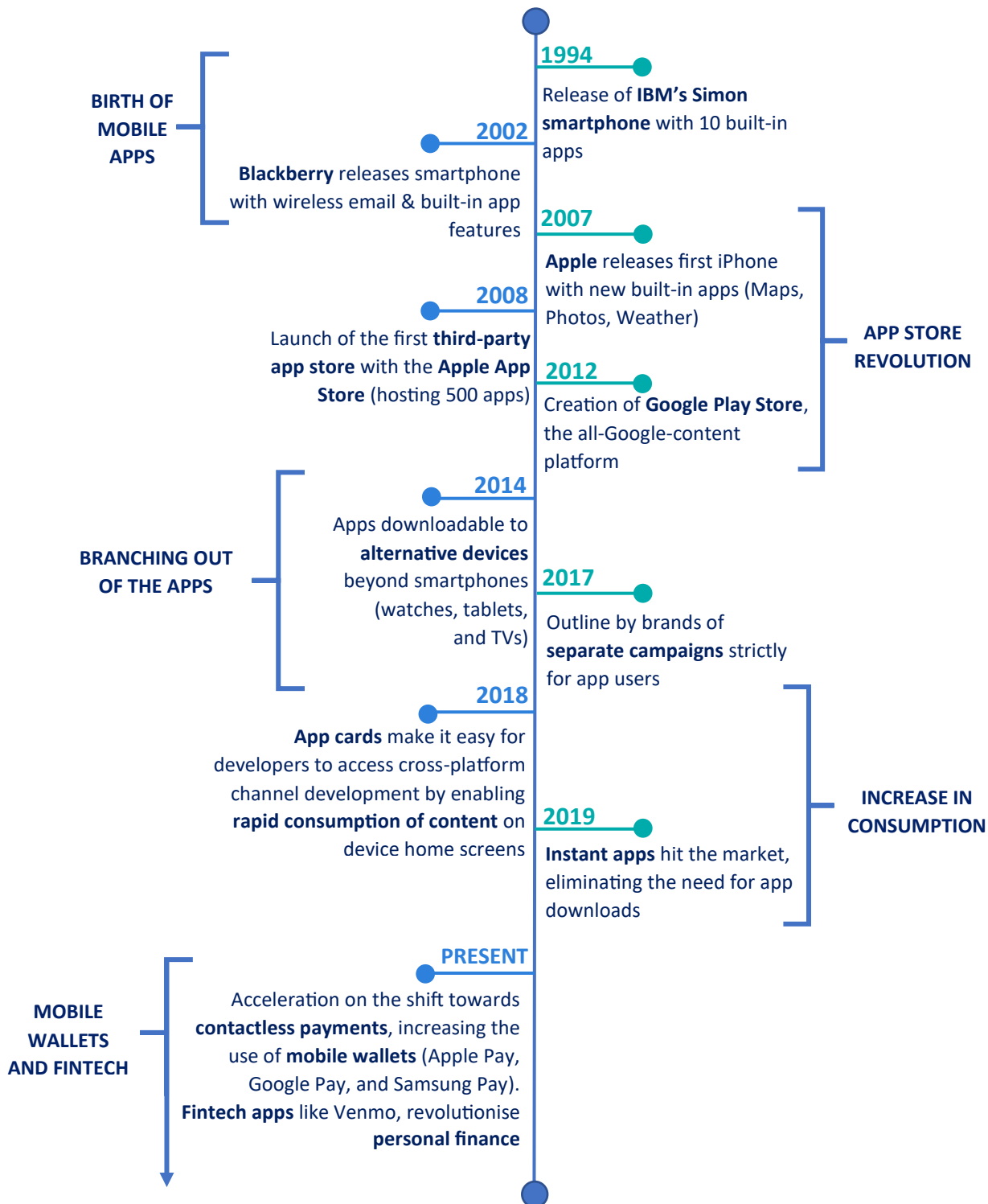
<sup>27</sup> Capitol Technology University (2021), [A Brief History of Mobile Apps](#), accessed on 15 May 2023.

<sup>28</sup> Matthew Panzarino (2014), [Foursquare's Swarm And The Rise Of The Invisible App](#), accessed on 15 May 2023.

<sup>29</sup> Ibid.

The following graphic is inspired by *Board Active Software* <sup>(30)</sup>.

Item 12. **Mobile app evolution timeline**



<sup>30</sup> Doug Pittman (2020), *A Brief History of Mobile Apps*, accessed on 15 May 2023.

Now, apps have reached the stage of revolutionary financial technology and mobile wallets, accelerating towards contactless payments everywhere and increasing the use of mobile wallets like Apple Pay, Google Pay and Samsung Pay, as well as financial technology (fintech) apps like Venmo and Bizum, among others. Amid this surge in fintech and mobile wallets, cryptocurrencies have also gained momentum, offering a decentralised and innovative approach to financial transactions beyond traditional systems. The increase in spatial computing competencies (e.g., augmented reality (AR), virtual reality (VR), mixed reality (MR), and artificial intelligence (AI) (see II.D.2)) as well as new trends like voice-enabled apps and blockchain-based apps, bring new avenues for potential legal use while also posing possible infringement risks<sup>(31)</sup>. Virtual reality, like the metaverse and its related devices, support apps<sup>(32)</sup>, giving users the ability to further customise the functionality and use of their devices<sup>(33)</sup>. Similarly, appliances that function through the internet of things (IoT devices)<sup>(34)</sup> facilitate remote monitoring and control and enable integration and automation of various functions, enhancing user convenience.

The possibility of future developments appears to be growing exponentially; in response, a proactive approach will be essential, involving continuous monitoring of technological developments, establishing solid legal frameworks, and developing effective strategies and tools for enforcement.

## II.B Widespread acceptance of apps

For a number of reasons, the use of mobile apps has rapidly expanded and gained widespread popularity. This rise was facilitated by increased smartphone adoption, better internet accessibility and speed, and improved user experience<sup>(35)</sup>. Demand for mobile apps increased as more users became aware of their advantages, sparking a boom in app development and the emergence of a vibrant app economy.

According to a study by Statista<sup>(36)</sup>, since the smartphone evolution, the annual growth in the smartphone user base has been within range of 0.3-0.6 billion. In 2016, the smartphone user count started at 3.6 billion, and in 2022, 6.6 billion smartphone subscriptions were reported, anticipating a growth in subscriptions by 2027 of 7.7 billion total, representing a 10.4 % growth in the user base growth annually.

---

<sup>31</sup> EUIPO (2022), [Study on the Impact of Artificial Intelligence on the Infringement and Enforcement of Copyright and Designs](#).

<sup>32</sup> Learn Crypto (2024), [My feed | Articles | What are the best Metaverse apps?](#), accessed on 12 February 2024.

<sup>33</sup> More information on all these technologies can be found in the EUIPO's [Intellectual Property Infringement and Enforcement – 2023 Tech Watch Discussion Paper](#).

<sup>34</sup> IoT appliances include, but are not limited to, home automation devices like smart refrigerators, smart locks, doorbells with sensors, smart thermostats, and smart kitchen appliances.

<sup>35</sup> Samar Patel, Mind Inventory (2022), [Mobile App Usage and Growth Statistics for 2023 and Beyond](#), accessed on 20 May 2023.

<sup>36</sup> Petroc Taylor, Statista (2023), [Number of smartphone mobile network subscriptions worldwide from 2016 to 2022, with forecasts from 2023 to 2028](#), accessed on 20 May 2023.

Developers can now reach users in more ways than ever before. The availability of many connected device types, like smartphones, smart TVs, and gaming consoles, has expanded the possibilities available to users, developers, and content producers globally, driving a significant and sustained increase in digital consumption across a range of services. Consumers have a number of options when considering the purchase of internet-connected devices. Users can access apps from many different sources (see III.B).

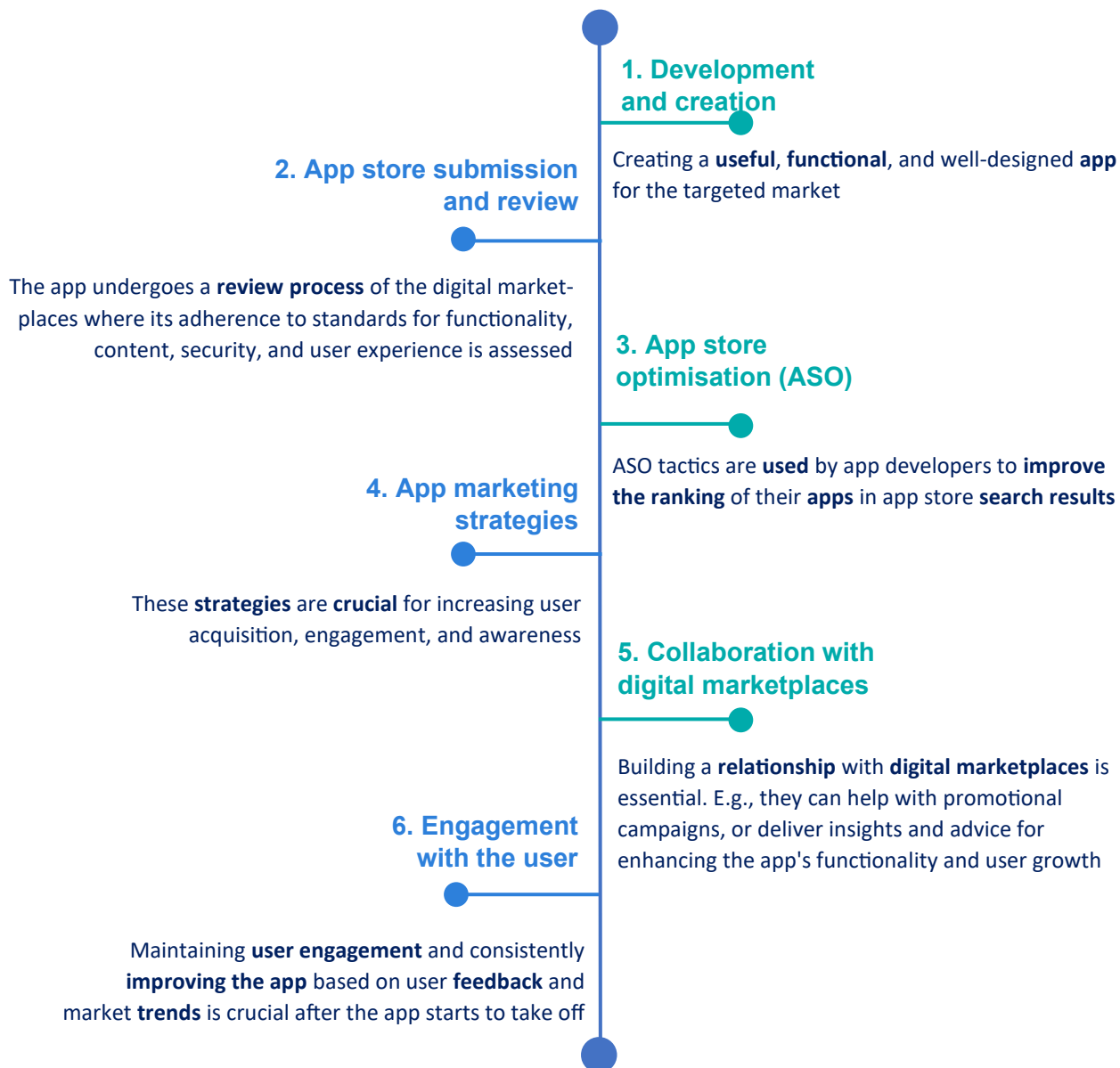
Beyond smartphones, the expansion of applications into the realms of smart TVs and gaming consoles has notably transformed the user experience, bringing a plethora of services directly to the comfort of the living room. Smart TVs now host a wide array of apps, ranging from streaming platforms to interactive fitness programs, enabling users to access a diverse mix of content without the need for additional hardware. Similarly, gaming consoles have evolved beyond their traditional role, functioning as comprehensive hubs where users can enjoy streaming services, social media, and web browsing in addition to the gaming functionality. This integration of apps into TVs and consoles has not only broadened the scope of digital entertainment but also created opportunities for developers to innovate and users to explore content.

When an app is commercialised, its popularity and success depend on efficient marketing tactics and partnership with market players. Within the creation and development phase of an app, developers will focus on creating a useful, functional, and well-designed apps for the targeted market. A review of the desired digital marketplaces is then conducted to ensure adherence to standards of functionality, content, and security, and to assess the user experience; this stage is referred to as 'app store submission and review'. App developers also take extensive measures to optimise their apps for app stores to improve rankings and search results and thereby increase traffic. This requires marketing strategies, which are crucial for increasing user acquisition, engagement, and awareness.

*The current app ecosystem includes a wide variety of apps that can be found on different platforms which can be challenging for combatting IP crime. For IP owners, it may be discouraging to see how easily IP-infringing apps can be published and disseminated – in just seconds – compared to the long processes needed to get them removed from the market. And even when removed, the developer may simply publish another app with the same functionality but with slight changes to the name, logo, or appearance. Developing and adapting apps is easier now than ever, especially with development kits, which are flooding the market.*

IP crime expert

### Item 13. Apps entering the business world



The development of technology, as well as the quick growth and widespread acceptance of apps, has been crucial in shaping the contemporary digital world. Both individuals and companies now have more influence, thanks to ongoing developments in mobile technology, internet connectivity, and app development frameworks. Since they provide solutions for communication, entertainment, productivity, and more, apps have become an important part of our everyday lives.

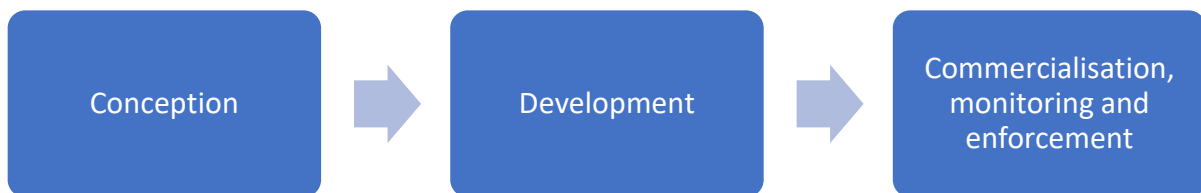
## II.C Exploitation of IP in app development

IP assets are a valuable resource in the social and economic development of nations and ecosystems <sup>(37)</sup>. The IP landscape has been significantly impacted by apps, both in terms of the exploitation and protection of IP.

Copyrights, trade marks, and trade secrets are important examples of IP that are frequently present in apps; notably, however, trade secrets are generally applicable to the practices behind the user interface of the app and pertain more to the app's developers or organisation. The ideas, concepts, designs, and software code used by developers to build apps may all be covered by IP regulations. The capacity to legally exploit IP in apps enables developers to profit from their work, encouraging innovation and promoting a thriving app ecosystem.

Within the lifecycle of an app, there are three main phases <sup>(38)</sup>, as depicted in the graphic below:

### Item 14. Life cycle phases of an app

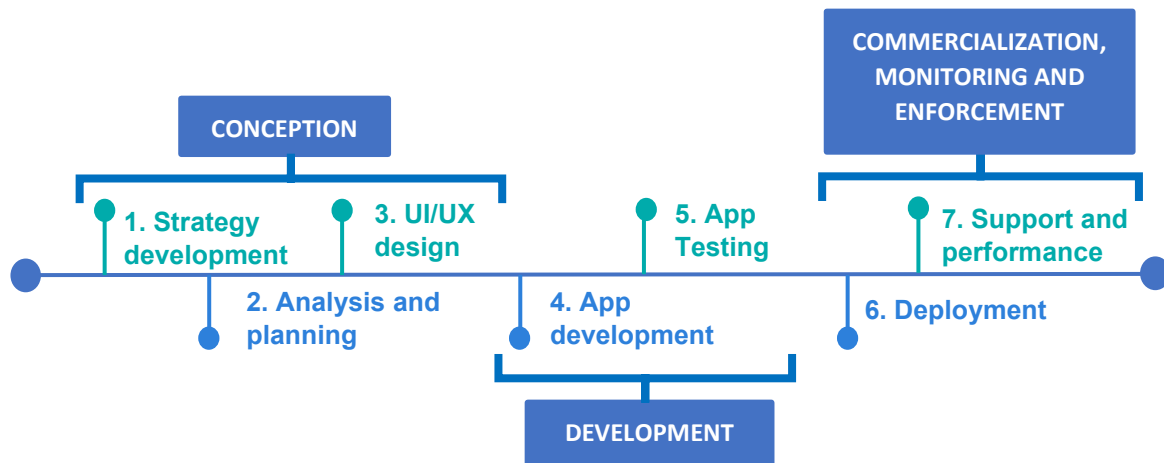


These three main stages apply to the 7-step process mentioned in the next section. Conception encompasses the strategy development, analysis, and planning and UI/UX design phases. App development and testing form part of the development phase. Finally, commercialisation, monitoring and enforcement come when the app is deployed and when developers receive support and performance analytics from users. This is illustrated in the chart below, showing the lifecycle of an app built on the previous model above.

<sup>37</sup> EUIPO (2021), [Pan European Awareness Campaign, World Anti-Counterfeiting Day 2021](#).

<sup>38</sup> A report developed by the World Intellectual Property Organization (WIPO) studies the role of IP in the development and commercialisation of apps. (2021), [The Role of Intellectual Property Rights in the Development and Commercialization of Mobile Applications](#), accessed on 6 June 2023.

Item 15. Life cycle phases of an app with the 7 steps of development



According to the report by WIPO, IP's role in the development and commercialisation of apps lies in the importance of defending the primary assets of app developers. While all types of IP can be considered, it is expected that copyright and trade secret protection will play a major role in the conception phase.

In the development phase, it has been established that IP including copyright and trade marks is significant in protecting the key intellectual assets (e.g. code, architecture, user interface, and design of user experiences) of a mobile app business, alongside the continued importance of trade secret protection.

At the pre-launch stage, protected innovations and design elements deserve special consideration.

In addition to any IP-related elements included in the commercialisation phase, it is crucial for an app business to adhere to the relevant regulatory regimes, like privacy and advertising rules, when the app is released.

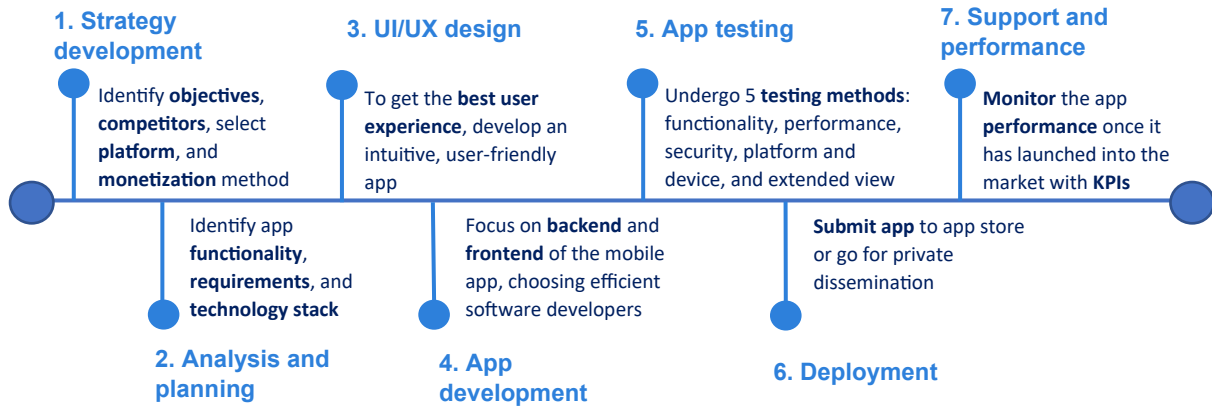
## II.D Developing and disseminating apps

### II.D.1 *Developing legitimate apps*

Both the technical specifications and business models have undergone major changes as a result of the introduction of apps. Although an app can be created through many different pathways, there are seven key steps that must be followed, listed below. This process has been developed to provide the key aspects to follow when developing an app. The following graphic was inspired by existing descriptions <sup>(39)</sup>:

<sup>39</sup> E.g., Mathew Carrington, Velvetech (2023), '[Mobile App Development Process: Ultimate Guide to Build an App](#)', accessed on 3 June 2023.

### Item 16. 7-step process for app development



The seven steps are described in more detail below<sup>(40)</sup>.

#### 1. Strategy development

- Identifying the main objectives that the app will pursue.
- Searching for existing or potential competitors.
- Platform selection is crucial, as this will have an effect on the ‘App development’ stage.
- In consumer apps, many options exist for monetisation, depending on the app developers’ goals.
  - In-app advertising: advertisements are displayed within the app, as native ads, banners, interstitials, or videos. Revenue is generated by charging advertisers for ad placements or by charging advertisers directly for ad placements or getting paid by ad networks facilitating ad placement for advertisers. Revenue models include payment based on impressions, clicks, or conversions.
  - In-app purchases: allowing users to access premium content, extra digital features, or virtual products through an app for a fee.
  - Subscriptions: offering users access to material or services in exchange for a recurring fee. As long as users maintain memberships, developers receive a regular income.
  - Affiliate marketing: third-party goods or services are promoted by developers or marketers, and commission is earned for each successful referral or transaction.
  - Paid apps: users are charged a one-time fee to download and use a paid app. Users pay up front to download the software, and developers profit from the first sale.

<sup>40</sup> E.g., Mathew Carrington, Velvetch (2023), ‘[Mobile App Development Process: Ultimate Guide to Build an App](#)’, accessed on 3 June 2023.



## 2. Analysis and planning

- Functional and non-functional requirements should be examined; particularly those actions within the app's software and system that impact the user experience.
- The definition of the app's roadmap to reach the set end goals is essential.
- Finally, the programming languages, tools, and frameworks that software engineers combine to create webs and apps are known as the 'tech stack', which can differentiate the app by making it available for only one platform, cross-platform, or multi-platform<sup>(41)</sup>.

## 3. User interface (UI)/ user experience (UX) design

- An app's design must receive a great deal of attention for users to have an excellent experience. Users will immediately migrate to rival products and stop using the tool if it appears to be messy or flawed. Therefore, the designs for the user interface (UI) and user experience (UX) must be intuitive and engaging and provide a seamless experience.

## 4. App development

- The creation of databases and server-side objects, which govern the app's performance, take place during the backend stage of app development. This is the point where the app's coding begins after selecting the correct programming languages. The hosting environment and database engines will also be chosen.
- The frontend of an app is where users will engage with it the most. To build it, there are three main methods.
  - Native: an app is created exclusively for each mobile platform, by fully optimising the code for each platform rather than being shared across platforms (i.e., the app is native to that platform). Although it can be more expensive, the increased speed, responsiveness, and the use of low-level software and hardware features may make it worthwhile.
  - Cross-platform: cross-platform apps are developed using a single codebase and deployed across multiple platforms. The code reusability and lack of limitation to a single operating system (OS) are significant advantages.
  - Hybrid: apps are developed using a combination of native-app and web technologies (e.g., HTML, CSS, and JavaScript). Developers write the code using web technologies and 'wrap' it in native-app capabilities that allow users to access the content through a web, mobile or cloud-based apps.

---

<sup>41</sup> Ayo Oladele, Velvetech (2023), '[Choosing the Right Tech Stack for Your Project: Basic Principles](#)', accessed on 3 June 2023.

- ‘No code’ app builders are tools, like software development kits (SDKs), that allow developers with limited technical knowledge to develop apps. These tools provide developers with the resources required to begin developing an app and contribute to apps being developed in a more standardised way (see more in III.A.2.a).

## 5. App testing

- An app may go through five testing procedures before release to ensure that it is reliable, secure, and bug-free.
  - **Functionality:** checking the app’s features and making sure everything functions properly.
  - **Performance:** paying attention to the app’s responsiveness, and how it responds to an increase in concurrent users while undergoing performance testing.
  - **Security:** data protection is of the utmost importance when developing enterprise solutions such as mobile insurance apps and healthcare apps, which operate in highly regulated industries. Security is of the utmost importance to ensure that they are not exposed to any vulnerabilities. Moreover, some additional marketplaces offer AI-based testing of apps security <sup>(42)</sup>.
  - **Device and platform:** the app must be up to date on compatibility, given the yearly release of new mobile devices and monthly operating system (OS) updates. Therefore, it needs to be tested using a variety of tools or simulators.
  - **Longer review:** the app must be tested with its end users before moving forward with deployment, gathering as much feedback as possible, whether this is by setting up focus groups or launching the software as a beta version.

## 6. Deployment

- Depending on the development platform, a variety of dissemination models can be used for deployment of the app into the market. The deployment approach for apps is straightforward: either submit the program to an app store or opt for alternative dissemination. Both major stores require the completion of several forms and the submission of the app for review.

## 7. Support and performance

- Apps should be managed consistently; to this end, key performance indicators (KPIs) must be followed, such as the number of app downloads, active users, average visit times, user lifetime value, ratings and reviews.

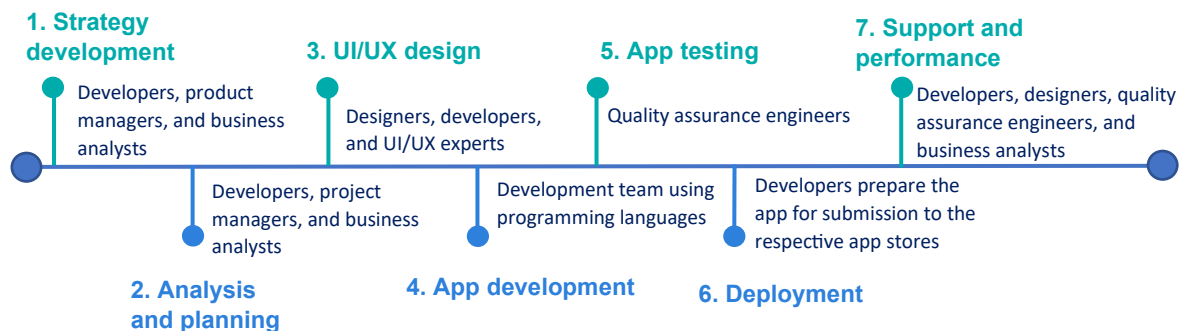
---

<sup>42</sup> This form of testing may either include on-device protection capabilities or cloud-based security solutions. On-device protection integrates on-device services with cloud components to consistently push functionality updates for device improvement. In the latter case, apps are scanned, using automated detection mechanisms and human security analysts, whether downloaded from the device app store or other channels. (From [Google Play Protect](#))

- Moreover, it is important to track crashes, bugs, user requests, and the overall performance of the app. In this way, the app improves over time.

Multiple stakeholders are involved at different stages throughout an app's development process. Each of these parties is essential to the effective creation of an app, contributing their knowledge and skills to guarantee that the finished product lives up to the expectations of both the company and the end users. The following depicts the most relevant stakeholders involved throughout the 7-step process.

#### Item 17. Actors involved in app development



- Project managers: in charge of supervising the entire development process, organising teams, establishing deadlines, and ensuring the success of the project.
- Designers: UI/UX designers focus on improving the entire user experience while creating aesthetically pleasing and user-friendly interfaces.
- Developers: programmers develop the app's code, implementing the necessary features and ensuring its function.
- Quality assurance engineers: before releasing the app to the public, they perform extensive testing to find and address any bugs or problems it might have.
- Product managers: are responsible for market research, strategic decision-making, and ensuring that the app is in line with the aims and objectives of the business.
- Business analysts: perform competition research, analyse market trends, and offer recommendations for decisions throughout the development process.

Depending on the complexity of the project and the resources available, each role can be filled by multiple people, or one person can fill multiple roles.

*What can sometimes occur is that a developer creates an app with a legitimate purpose only to realise that they can earn more money with an IP-infringing business model simply by changing a few functionalities of the app.*

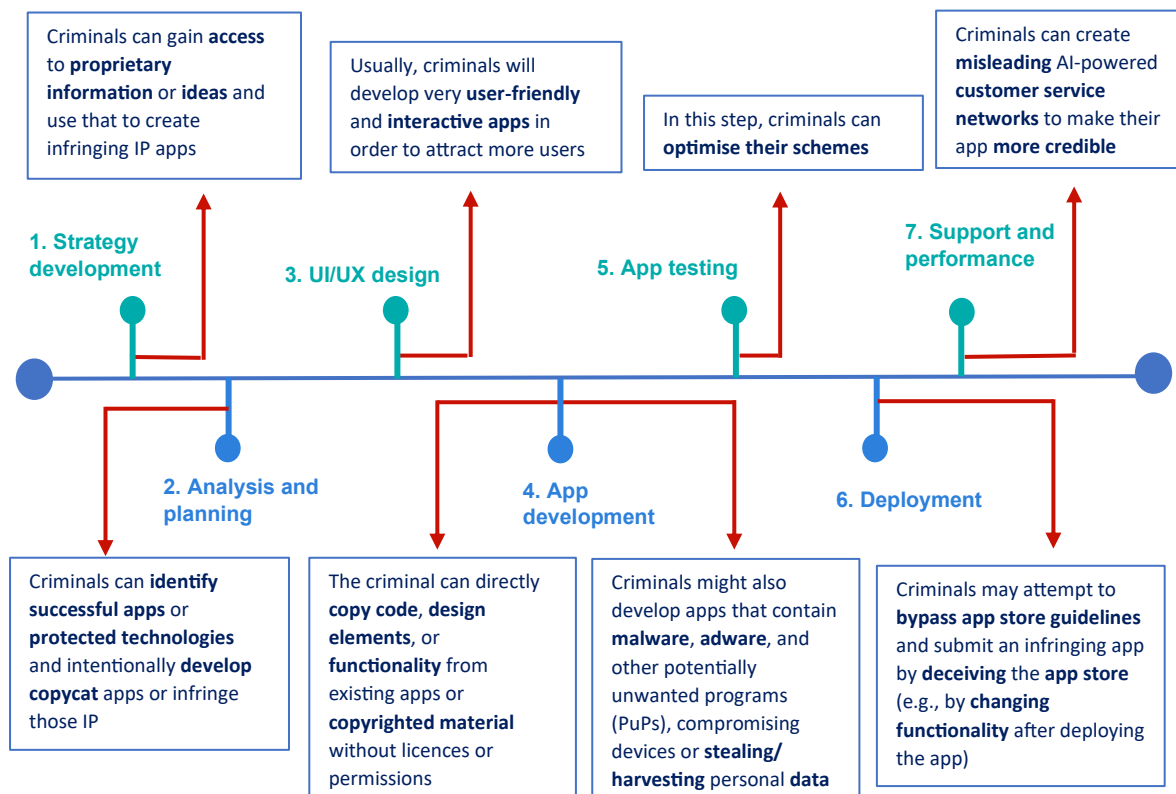
IP crime expert

## II.D.2 Developing IP-infringing apps

An IP criminal may intervene at any stage in an app’s development to produce an IP-infringing app.

There are several instances in which an IP criminal can perpetrate IP infringement (for each of the seven steps):

### Item 18. Criminal-infiltrated 7-step process for app development



1. Strategy development: IP criminals may have access to proprietary information and use that to infringe IP (e.g., through trade secret theft).
2. Analysis and planning: IP criminals can identify successful apps or protected technologies and intentionally develop copycat apps or infringe existing IP.
3. User interface (UI) / user experience (UX) design: IP criminals develop user-friendly and intuitive apps to attract more users.
4. App development: IP criminals can directly copy code, design elements, or functionality from existing apps and copyrighted material without licences or permissions. They may also change the source code of apps to covertly include malicious or fraudulent functionalities that may be used for IP infringement.
5. App testing: IP criminals may optimise their schemes.

6. Deployment: IP criminals may attempt to deceive app stores and bypass app store guidelines (e.g., changing functionality after deploying the app).
7. Support and performance: criminals can create misleading AI-powered customer-service networks to make their app appear more credible.

All the above steps can easily be carried out by an automated artificial intelligence (AI) model (see Item below). AI models specialised in generating malicious or otherwise illegal code are readily and cheaply available on the dark web (see III.A.2). Models may even be trained on the basis of unlawfully ingested training sets, or data uploaded without permission or authorisation, as well as malicious and fraud-related data. Additionally, generative AI models such as generative adversarial networks (GANs) can produce new data of any kind that have the same properties and quality as IP protected data.

*An emerging threat is that there are ever lower entry barriers for criminal app developers due to the use of artificial intelligence (AI) and crime-as-a-service (CaaS) providers. New criminal operators therefore do not necessarily need coding skills anymore to create apps of scale.*

IP crime expert

#### Item 19. Important emerging trend – artificial intelligence (AI)

### Important emerging trend: artificial intelligence (AI)



Artificial intelligence (AI) is the simulation of human intelligence in machines programmed to perform tasks that typically require human cognition, such as learning, problem-solving, perception, and decision-making. AI algorithms use advanced statistical and mathematical techniques to process large amounts of data and identify patterns and relationships that can be used to make predictions or inform decisions. AI technology is rapidly advancing and is being applied in a wide range of industries, from healthcare and finance to transportation and entertainment, with the potential to revolutionise the way we live and work. However, there are also concerns about the ethical and societal implications of AI, particularly around issues such as bias, privacy, and job displacement.

As a tool for criminality, especially the availability of illegal AI services on the dark web (see III.A.2) is worrying. Read more about the misuse of AI for IP-infringing purposes in the EUIPO 'Study on the impact of artificial intelligence on the infringement and enforcement of copyright and designs' <sup>(43)</sup>.

<sup>43</sup> EUIPO (2022), '[Study on the impact of artificial intelligence on the infringement and enforcement of copyright and designs](#)'.

Within the realm of apps and IP crime, some IP criminals also have the capacity to provide development of apps as part of crime-as-a-service (CaaS) (see III.A.2.a) to aid newcomers to IP crime in specialising in apps related to IP-infringement.

Both the application of AI models and CaaS mean, in practical terms, that the entry requirements both technically and financially for engaging in IP crime enabled by apps is relatively low and continuously is becoming lower.

Information on development of apps with focus on each business model here:



- Infringing Business Model 1: infringement of copyright-protected content (see III).

- Infringing Business Model 2: marketing of IP-infringing physical goods through apps (see IV).



- Infringing Business Model 3: IP infringement for malicious and fraudulent purposes (see V).

- Infringing Business Model 4: trade secret theft (see VI).



### II.D.3 *App gateways*

Apps can be disseminated through various app brokers (e.g., official app stores, app marketplaces and open app stores, see III.B.1) and other types of gateways (e.g., direct downloads and downloading various unauthorised sources, see III.B.2).

App stores and marketplaces generate revenue from having apps available, including through:

- developer fees to marketplaces,
- direct income to the app store from advertisements;
- income per download, if it is a paid app;
- in-app advertisements;
- funnelling users to premium monthly subscriptions.

Each app broker typically establishes their own standards to govern their app ecosystem, in an attempt to create a compliant, secure, and safe environment for businesses and users (see III.B.1).

Generally, IP criminals have an interest in bypassing precautionary, preventive, and proactive measures. In certain situations, such as, direct download and downloading from various unauthorised sources (see III.B.2), such measures might be bypassed or fully avoided, and versioning might also be applied (see IV.A.3).

Information on app brokers and other gateways of app delivery for each business model here:



- Infringing Business Model 1: infringement of copyright-protected content (see III).

- Infringing Business Model 2: marketing of IP-infringing physical goods through apps (see IV).



- Infringing Business Model 3: IP infringement for malicious and fraudulent purposes (see V).



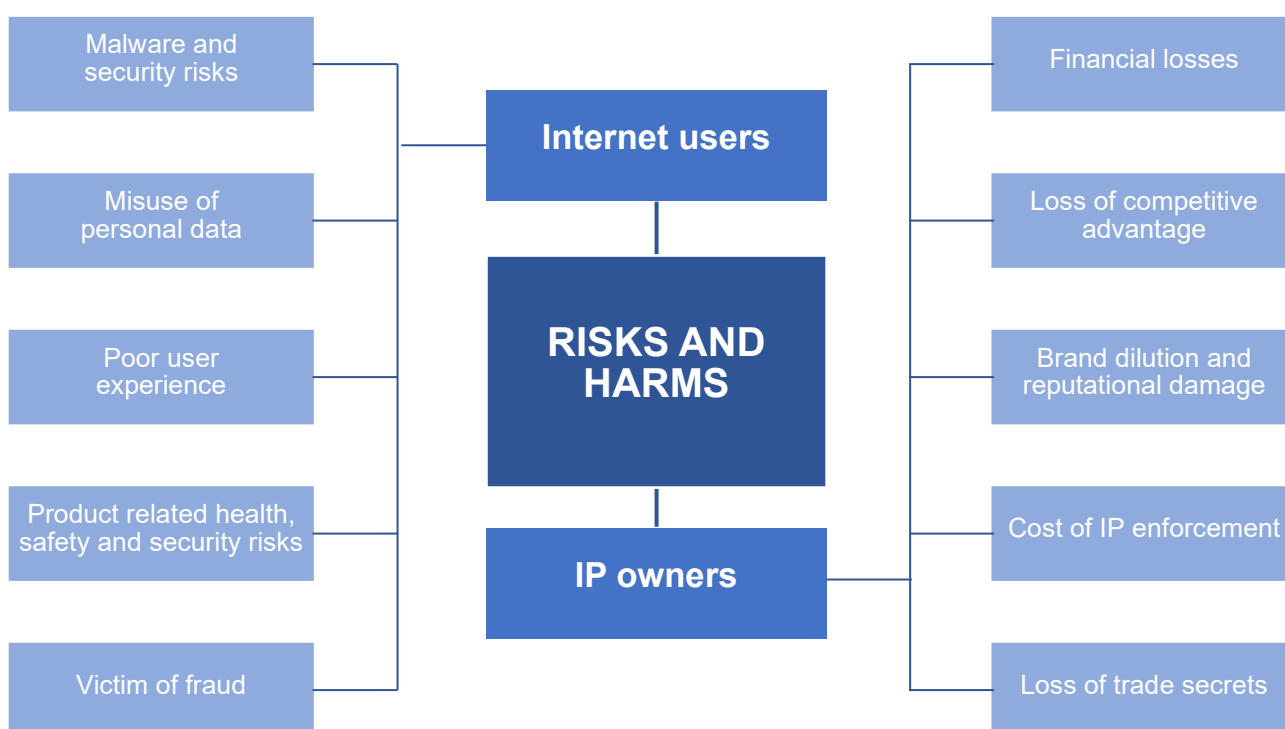
- Infringing Business Model 4: trade secret theft (see VI).



## II.E Risks and harm

There are a number of serious risks and harms connected to IP crime enabled by apps.

### Item 20. Risks and harms of IP crime



### II.E.1.a Internet users

Rather than conducting illegal activity through websites, IP criminals committing crimes through apps can have more control over internet users' behaviour and data. Through apps, the IP criminals can lock users in and track their movements more precisely, while gradually requesting more permissions as the user engages with the app.

Specific direct threats to internet users include the following:

- **Malware and security risks:** IP-infringing apps carry an increased risk of malicious software which can potentially compromise users' security systems and device integrity (see V). In some cases, even if deleted, the harm can linger on a user's device.



- Misuse of personal data: IP-infringing apps can access users' personal data and put them at risk of identity theft. IP-infringing apps may also be used for extortion, impersonation or as training data for AI models (see II.D.2). Moreover, IP-infringing apps may be used to collect data from other apps installed on the device as well as environmental telemetry, such as GPS, temperature, speed, and microphone or camera recording to facilitate surveillance.
- Poor user experience: IP-infringing apps are usually not bound to the same standards of quality or customer service as legitimate apps, which may result in insufficient software maintenance. Without these standards, the service may be less reliable and diminish the user experience.
- Exposure to dangerous or sub-standard IP-infringing goods: Internet users might be exposed to marketing of IP-infringing goods that can pose health, safety and security risks (see IV).
- Victim of fraud: malicious and fraudulent apps might expose internet users to fraudulent schemes aiming at obtaining unwarranted financial advantages from the internet user (see V).

*The way potential customers use mobile phones, and the internet has changed. Apps facilitating IP infringement react to these changes of behaviour very quickly and respond, even if we cannot see it.*

IP crime expert

### II.E.1.b IP owners

IP owners are exposed to various risks as a result of IP infringement, including:

- Financial losses: IP owners might incur financial losses due to unauthorised marketing of IP-infringing goods or services, including the availability of unauthorised copies of their apps. Read more about copyright infringing digital content (see III) and marketing of IP-infringing goods (see IV).
- Brand dilution and reputational damage: the reputation of IP owners may be heavily impacted if associated with infringing apps that expose users to malicious or fraudulent practices (see V) and poor user experience as overall brand confidence may decline.

*When investigating IP crime facilitated by apps, it's easier to get law enforcement agencies involved if solid preparatory work has been done by the private sector in which as much evidence has been collected as possible.*

IP crime expert

- Cost of IP enforcement: IP owners must dedicate time, effort, and resources to monitoring and enforcing their IP against infringing apps, distracting them from core operations in terms of both time and money.
- Loss of competitive advantage: IP infringement may, in connection with the previously mentioned risks and harms, cause damage to the competitive advantage of IP owners including when their carefully developed apps are duplicated.
- Loss of trade secrets: IP owners may experience losses due to theft and exposure of confidential business information (see VI).

Item 21. **Enforcement and investigative measure – criminal referrals**

## Enforcement and investigative measure: criminal referrals



The *Intellectual Property Owner Guide to Criminal Referrals in Intellectual Property Crime Cases* <sup>(44)</sup> sets out a roadmap to assist IP owners who choose to refer cases involving the infringement of their respective IP to investigating authorities for criminal enforcement.

The guide is designed to be a practical, IP owner-focused tool to assist all IP owners in making a criminal referral of an infringement of their IP. The guide focuses on serious and often organised crimes involving trade marks, copyright and trade secrets. The special focus on trade marks, copyright and trade secrets reflects that these IPs are the most common in criminal proceedings.

A successful criminal investigation and subsequent prosecution of an IP crime depends, in a meaningful part, on substantial assistance from IP owners. Often, the IP owner is the first to notify investigating authorities of an IP crime – and that notification typically comes in the form of a criminal referral.

An important purpose of the guide is to make it easier for IP owners to provide important information to investigating authorities as part of their criminal referral. The guide assists IP owners on how to conduct a preliminary investigation of an IP infringement in preparation for a criminal referral as well as how to prepare the criminal referral itself. In addition, the guide offers specific advice tailored to the three most common IP crimes: criminal trade mark counterfeiting, criminal copyright piracy, and trade secret theft.

The guide also provides sections intended to help IP owners understand their role after a public investigating authority has received a criminal referral and decided to open a criminal investigation. Moreover, the guide includes a helpful annex with checklists for IP owners to use when reporting a trade mark crime, criminal copyright infringement, and criminal trade secret theft.

The guide was developed as part of the EMPACT framework (see footnote 20).

<sup>44</sup> EUIPO (2024), '[EMPACT Intellectual Property Owner Guide to Criminal Referrals in Intellectual Property Crime Cases](#)'.

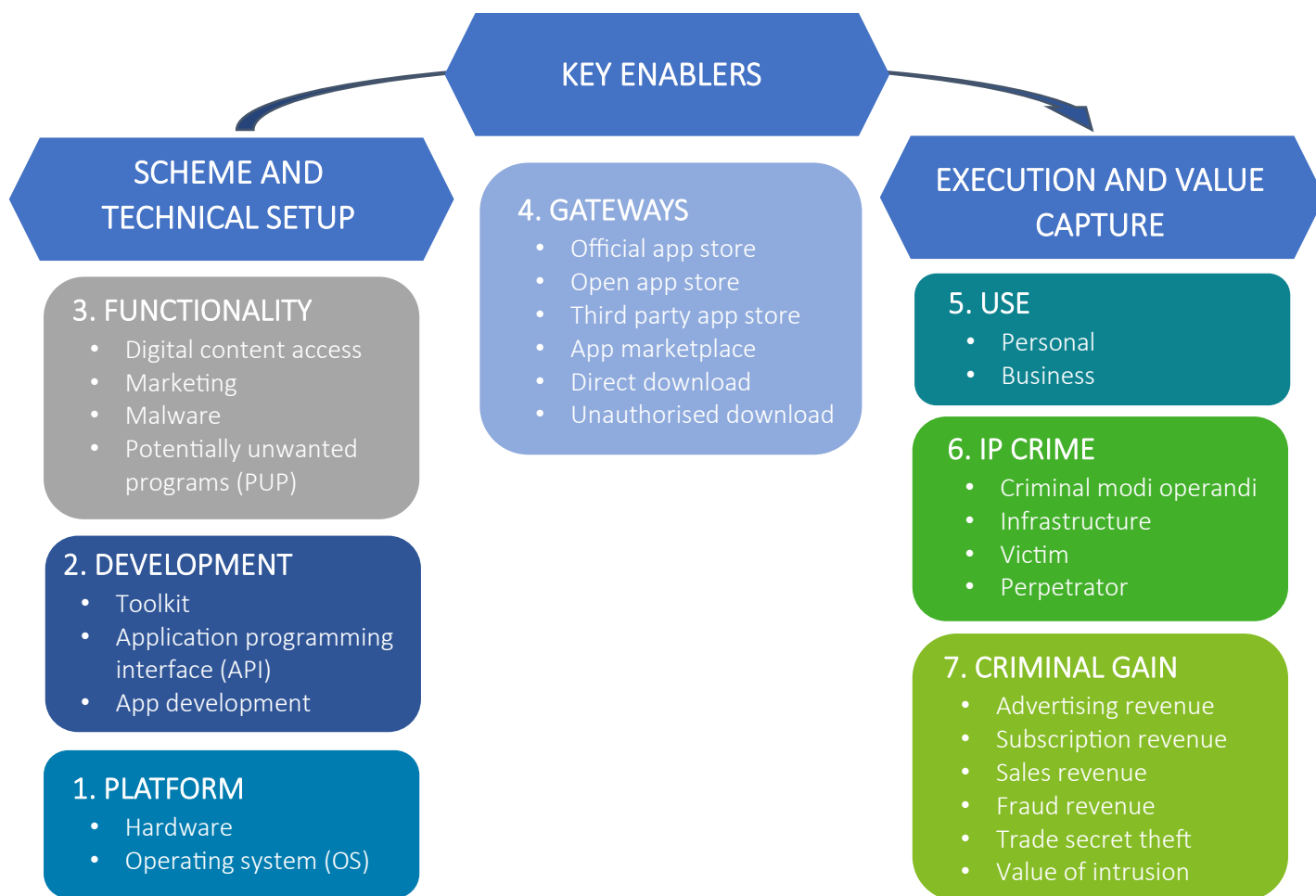
### III Infringing business model 1: infringement of copyright-protected digital content



In an increasingly digital ecosystem, the infringement of copyright-protected digital content is a phenomenon gaining user traction.

The description of the business models follows the content of *the arc of IP crime related to apps*. The business models described in relation to infringement of copyright-protected digital content has some overlaps with business model 3 related to fraudulent and malicious IP crime (see V).

#### Item 22. *The arc of IP crime related to apps*



## III.A Scheme and technical setup



The scheme and technical setup of an IP crime refers to the methods and instruments used by IP criminals to infringe IP. In the first business model, specifically infringing the IP related to copyright-protected digital content, the method, content source, and setup that criminals use to infringe the IP of the owner of digital content, such as music, movies, software, books, software, and databases are all part of the overall scheme. The IP criminals use a variety of techniques to reproduce and disseminate copyright-protected digital content, usually with the aim of generating profit through subscription revenue or income generated by advertising.

The technical setup can involve a variety of actions, beginning with the choice of one or more platforms used to perpetrate the crime, the development of the IP-infringing apps, and defining and developing the app's functionality, focusing on how to reproduce and disseminate the content.

### III.A.1 Platform

The platform for IP infringement of copyrighted digital content describes the various channels and methods through which criminals can disseminate copyrighted digital content without authorisation from the IP owners. In terms of apps, their platform may expand beyond the smartphone sector to reach all connected devices, including TV sets with TV manufacturers' built-in operating systems (OS) (or other open-source operating systems) allowing the user to access apps. The modern smart TVs allows users to download apps from an app store (either the manufacturers or third-party app stores) and build on top of smart TV functionalities like spatial gesture input and speech recognition. Apps can also be used on TV sets through gaming consoles, firesticks, or similar devices.

Across all platforms, IP criminals may attempt to take advantage of the hardware developer through flaws or vulnerabilities in the hardware or software when developing an IP-infringing app. They do so by exploiting security flaws, reverse engineering the hardware or software, or making unauthorised modifications.

On the other hand, the organisation that creates and supports the operating system on which apps are run is known as the operating system (OS) provider. OS providers are in charge of managing the hardware resources, granting access to system services and application programming interfaces (APIs), managing the user interface, and providing the fundamental functions. When creating an app that infringes IP, an IP criminal may try to take advantage of the OS provider by working around the rules that the provider has put in place to stop IP infringement. An example of this would be exploiting zero-day vulnerabilities in the OS used<sup>(45)</sup>. Other ways in which IP criminals may exploit OS providers are the following.

---

<sup>45</sup> IBM, [What is a zero-day exploit?](#), accessed on 14 December 2023.

- Giving misleading information: in order to have their app accepted on the platform of the operating system (OS) provider, an IP criminal may attempt to falsely portray their app or its capabilities, to the point where they may alter the functionality of the app to make it seem as if it does something completely legitimate and different from what it actually does.
- Unauthorised use of third-party IP: unauthorised use of IP belonging to a third party is possible, as are efforts to publish a program on the platform of the operating system (OS) provider without revealing or getting the required licences. An example is the Trezor app (see V.C.2 in which the case is addressed), that was published in the app stores and was available to all users and took advantage of IP.

In each of these scenarios, the developer of the operating system may take steps to stop the illegal app from being released or disseminated on their system. This can entail taking the app down from the platform, banning or revoking the developer's account, or even taking legal action against the offender.

### Item 23. Case example - App piracy group

#### App piracy group

This App Piracy Group case marks the first time that website domains concerning cell phone app marketplaces were seized by law enforcement authorities<sup>(46)</sup>. The United States' Department of Justice (USDOJ) executed seizure orders against the domains [applanet.net](#), [appbucket.net](#) and [snappzmarket.com](#) for the illegal distribution of copies of copyrighted Android mobile apps.

The individuals believed to be leading these piracy groups were charged with criminal copyright infringement and conspiracy to commit criminal copyright infringement, due to their large-scale violation of IP. The groups behind [snappzmarket.com](#) and [appbucket.net](#) were each found to have reproduced and distributed over one million copies of copyrighted Android mobile, through their own alternative online markets. The larger [applanet.net](#) group was found to have reproduced and distributed over 4 million copies of copyrighted Android mobile device apps, with the retail value of over \$17 million, on their alternative online marketplace.

In total, nine members across the three different groups were convicted; two members of the SnappzMarket group were arrested<sup>(47)</sup>. The sentencing of the individuals ranged from probation to 46 months in jail<sup>(48)</sup>.

The operation was a coordinated effort involving Dutch and French law enforcement officials. The case underscores the seriousness with which digital copyright infringement is treated by law enforcement agencies. It was the coordinated efforts between law enforcement agencies, both domestic and international, that led to the successful prosecution of these individuals.

<sup>46</sup> US Department of Justice (2012), [Federal Courts Order Seizure of Three Website Domains Involved in Distributing Pirated Android Cell](#), accessed on 16 January 2024.

<sup>47</sup> US Department of Justice (2014), [Leader and Co-Conspirator in Android Mobile Device App Piracy Group Plead Guilty](#), accessed on 16 January 2024.

<sup>48</sup> US Department of Justice (2016), [Fourth Conspirator in SnappzMarket Android Mobile Device App Piracy Group Convicted of Conspiracy to Commit Criminal Copyright Infringement](#)", accessed on 16 January 2024.

### III.A.2 *Development*

Building on the previous chapter on developing IP-infringing apps (see II.D.2), this section will explore the subject of app development further.

A deep technical knowledge and understanding is no longer a challenge; development is easy as long as the IP criminals have the capital to pay for the initial setup, or the ability to learn the skills needed to develop an app. Knowledge varies depending on the IP criminal and on whether there are enough resources and people willing to facilitate crime-as-a-service (CaaS) (see III.A.2.a) and sell copyright-protected digital content. The dark web is a platform that can be used to facilitate CaaS by providing IP criminals with a shield of anonymity when conducting their operations. Therefore, even if an IP criminal has limited technical insight, apps can be developed relatively easily, after which the IP criminal can run a service that infringes copyright-protected digital content. To help an IP criminal with limited technical skills, toolkit developers, app developers and application programming interfaces (APIs) can all assist in IP infringement.

#### Item 24. Important emerging trend – dark web

##### Important emerging trend: dark web



Dark web<sup>(49)</sup> is a term describing a certain part of the internet, usually considered part of the deep web which is the unindexed part of the internet consisting of data that cannot be indexed by traditional search engines and is therefore not directly searchable. In popular terms the dark web is specifically designed to secure the anonymity of those who disseminate information or who carry out other activities by making use of specific technologies and network configurations. As a result, specific software and/or configurations are needed to access dark web resources and websites.

One of the most popular networks forming the dark web is the onion router (TOR) network. The TOR operates through a network of connected nodes where all communication is highly encrypted and obscured through multiple connected geographically distributed nodes. The network can be used to access traditional internet resources but also services and websites only available via the TOR network. These dark web resources are often dedicated to criminal activity and payment options are mostly cryptocurrencies. The dark web can be used to infringe IP in a multitude of ways, including the use of dark web marketplaces for marketing IP-infringing products, sales, or disclosure of trade secrets, and as a platform for developing illegal apps, intrusion tools, and malware. Additionally, the dark web can facilitate anonymised communication and interaction between IP criminals, programmers, and providers of crime-as-a-service (CaaS) (see III.A.2.a).

Some artificial intelligence (AI) (see II.D.2) tools present themselves as an alternative designed for malicious and fraudulent purposes. They may even be trained on the basis of unlawfully ingested training sets, or data uploaded without permission or authorisation, as well as malicious and fraud-related data.

<sup>49</sup> See more on the dark web in the EUIPO's '[Research on Online Business Models Infringing Intellectual Property Rights – Phase 1](#)' (2016).

### III.A.2.a Toolkit

Software development kits (SDKs), application programming interfaces (APIs), code libraries, artificial intelligence (AI) (see II.D.2) using for example natural language processing (NLP), are some of the resources and tools that toolkit developers offer to app developers. Through some app stores and marketplaces, users can download official app Android Package Kits or Android App Packages (also known as an APK file), which include all the components an app requires to successfully be installed on a device <sup>(50)</sup>.

The SDK in particular provides developers with most, if not all, of the resources needed to build software or an app (i.e., inter alia, code samples, testing and analysis tools, developer documentation, and debuggers). The benefit of SDKs is that they enable software developers to build software applications in a more efficient and standardised way <sup>(51)</sup>.

These technologies can make it simpler and more effective for app developers to construct and improve their apps <sup>(52)</sup>, for example by allowing cross-platform mobile development.

However, IP criminals may still take advantage of these tools in order to create IP-infringing apps without being experts in the matter by hiring developers to engage in crime-as-a-service (CaaS) (see III.A.2.a). For example, criminals can download APL files to test and analyse them in order to reproduce the design and functionality. In addition, SDKs often provide an emulation environment for such purposes, specifically that a user can run any APK files on any selected emulated device types.

---

<sup>50</sup> Ben Stegner (2023), [What Is an APK File and What Does It Do? Explained](#), accessed on 4 June 2023.

<sup>51</sup> IBM Cloud Education (2021), [SDK vs. API: What's the difference?](#), accessed on 13 March, 2023.

<sup>52</sup> Ibid.

## Item 25. Important emerging trend – crime-as-a-service (CaaS)

### Important emerging trend: crime-as-a-service (CaaS)



Cyber-attacks are challenging to investigate given that they contain multiple steps from the initial intrusion<sup>(53)</sup> and often entail multiple actors working on parts of the criminal process, which is an important dimension of: crime-as-a-service (CaaS)<sup>(54)</sup>. Cybercrime services are widely available and have a well-established online presence, with a high level of specialisation inside criminal networks and collaboration between illicit providers. The illicit service providers cater to a large number of criminal actors by offering monitoring, delivery, and obfuscation services. Such services are often offered for sale or advertised on dark web forums and marketplaces. Closely connected to CaaS is bulletproof hosting services<sup>(55)</sup> where criminals can rent digital infrastructure including hosting services that generally accept that the infrastructure is used for criminal purposes and avoid collaboration with law enforcement.

Cyber-attacks are expected to increase as a criminal threat affecting the EU<sup>(56)</sup>. The CaaS ecosystem will further develop in order to service a wider criminal base. Cybercriminals are also able to further embrace new technologies and maximise the reach of their services, with sensitive data as a core target, such as in apps as per the following examples:

The international law enforcement action named ‘Operation Vaccination’ took down a mobile malware that was distributed to users by an app, FluBot, which was first spotted in December 2020 and which gained traction and compromised a huge number of Android devices worldwide. The malware was installed via text messages which asked users to click a link and install an application to track a package delivery or listen to a fake voice mail message. Once installed, the malicious application, FluBot, would ask for accessibility permissions. The hackers would then use this access to steal banking app credentials or cryptocurrency account details and disable built-in security mechanisms. This strain of malware was able to spread like wildfire due to its ability to access an infected smartphone’s contacts and its ability to self-replicate.

Another operation named ‘Operation Power Off 3’, as part of an international effort against DDoS service providers, took down some of the world’s biggest booter services, designed to enable users to launch crippling DDoS attacks against critical online infrastructure.

In a similar vein, in 2022, a prolific cybercriminal was under investigation for having created and sold RacoonStealer, a data theft malware in existence since 2019. The malware was sold as a service to other criminals for a subscription fee of USD 200 per month to be paid in cryptocurrencies. The malware was believed to have been used to steal personal data through browsers, apps, and cryptocurrency wallets.

### III.A.2.b App programming interfaces (API)

App programming interfaces (APIs) are collections of tools and protocols that facilitate communication between two platforms such as social media networks, payment processors, and other third-party services. APIs are often included within SDKs and usually consist of the interface itself and technical specifications and documentation, which give information on how to integrate the APIs<sup>(57)</sup>. APIs are an essential element of connecting software applications and allowing for information to be relayed between programs. If an API has been improperly designed or does not use the best practices for IP infringements, it may result in IP

<sup>53</sup> The initial intrusion may be executed via lateral movement or privilege escalation, or data exfiltration and exploitation.

<sup>54</sup> EUROPOL (2023), ‘[Internet Organised Crime Assessment \(IOCTA\)](#)’, accessed on 4 April 2024.

<sup>55</sup> Ibid.

<sup>56</sup> Ibid.

<sup>57</sup> See footnote 51.



infringements, such as the illegal use of another party’s confidential information or copyrighted content<sup>(58)</sup>.

API abuse can be seen with specifically branded media players, particularly in the music sector. Although they are legitimate, some malicious individuals may take advantage of the app’s success by using the name of the app without authorisation, developing modified versions to disseminate through third-party app stores and websites. These unofficial versions may feature altered APIs that permit the apps to stream copyrighted films and TV shows without the required consent from the IP owners. Copyright infringement issues result from the updated APIs allowing the infringing apps to access and broadcast unlicensed content from outside sources.

### III.A.2.c App developers

App developers may take advantage of tools that are already generated, or pre-existing code, and build apps. There are existing tools, such as software development kits (SDKs) that allow app developers to develop apps (see III.A.2.a). If developers are experts and create the code for their apps, they may sell it in order to generate profit. Ultimately, the app development process requires a certain level of experience and access to specialised tools (see III.A.2.c).

New developers have created an online phenomenon called ‘Robin Hood pirates’, where they like to share their knowledge and post among themselves about how they can break into systems and create brand-new apps that share infringing content for no monetary gain. To fund their operations, these new developers will often receive donations from other users in the community or crowdfund their projects. If unable to adequately finance their app, they may still offer it free of charge, and they will often be powered by donations from other users within their community.

*‘Robin Hood pirates’ are groups of young developers, quite often underage, who like to share their knowledge and post among themselves how they can break into a system and create new apps. They sometimes commit IP crime, not primarily for monetary gain, but for reputation.*

IP crime expert

---

<sup>58</sup> See footnote 51.

Item 26. **Enforcement and investigative measure – reverse engineering**

### Enforcement and investigative measure: reverse engineering



Just as IP criminals can reverse-engineer legitimate apps, reverse engineering can also be used as an investigative measure. Through reverse engineering, the investigator will dissect and scrutinise the internal workings, functionalities, and security features of an app. For example, apps developed with poor security standards may be easy to investigate using reverse engineering.

Reverse engineering techniques and methods <sup>(59)</sup> include the following:

- analysis of the app's code without executing it, this static analysis can reveal important information, including related to security and encryption features;
- decompilation, also known as disassembly for personal computers helps to analyse the source code and other important parts of the app, including digital identifiers;
- tracing, intercepting or augmenting function calls, which make it possible to understand the functionality of the app;
- dynamic analysis carried out in an often isolated or sandboxed environment where the app code is executed, and the behaviour of the app is detected.

Using reverse engineering methods, the investigator can gain insights into the modus operandi of the criminal activity and identify similarities and connections to other apps and websites.

Reverse engineering can be an effective tool in applying the 'follow the pattern' investigative strategy, which aims to join together what appear to be separate and isolated digital phenomena but are actually parts of the activities of the same individual or criminal group and disclose the true scope of the enterprise. It might therefore be possible to connect different apps to each other and/or to other online activities.

By misusing infrastructure providers that are intended to maintain a secure internet, app developers can try to protect their anonymity at all costs, hiding the location of their infrastructure. Therefore, law enforcement agencies, IP owners and businesses cannot track their location, complicating the investigation to close them down.

Platforms and tools that may be used in the creation of IP-infringing apps may also be considered liable for promoting IP infringement. Even if the platform is not found to be infringing IP itself, as in the Xstream Codes case below, law enforcement agencies from the relevant countries may censor the platform.

### III.A.3 *Functionality*

The ability of apps to give users access to various sorts of digital content is referred to as 'digital content access'. In this case, it may be deemed IP infringement if an app grants users' access to copyright-protected content without authorisation.

A current problem with app functionality is that criminals have discovered they may be able to modify their apps after they have been accepted on app stores and disseminate them through

<sup>59</sup> Rico, Anthony, [Mobile App Reverse Engineering: Tools, Tactics and Procedures](#), accessed on 12 February 2024.

other gateways (see IV.A.3 on versioning). As a result, IP criminals create seemingly legitimate apps, receive approval by app stores, and then alter their functionality to include content that infringes IP. These changes in functionality can lead to various forms of IP infringement.

Other functionality challenges are the following.

- Illicit digital content access: criminals give users access to infringing digital content. This content can be disseminated in various ways: for example, an app can represent a book author's content in the form of test questions without obtaining authorisation from the IP owner. The app would simply include passages from the book and reading-comprehension-like multiple choice questions for the app user to interact with.
- Infringing developers can apply geo-blocking techniques, where infringing content is only shown in targeted countries, or blocked from being installed in another country, as an obfuscation technique. An example would be where, in the case of a provider in one country, the app is not available in that country, but only where the target audience is located. In addition, it is also possible to limit the version of the operating system or device types where the app can be installed. IP criminals may also block the use of VPNs and/or use an emulator. Doing so allows the IP criminal to avoid copyright infringement lawsuits and guarantees a more regulated dissemination of the illicit content, boosting their earnings and reducing the possibility of law enforcement finding them and shutting them down.
- Apps blocking the screenshot functionality: restricting users from taking screenshots while using the app may be a feature of some infringing apps. By preventing users from taking and sharing screenshots of copyright-protected content, they hope to make it more difficult for the copyright owners to detect and report infringement.
- Apps that hide the identity of the IP criminal: IP criminals operating apps may hide their identity under several layers of anonymity by using VPNs to conceal their location, using encryption tools, proxy servers and the dark web. IP criminals may also fabricate accounts and identities in order to operate under pseudonyms, making it more difficult for law enforcement to connect their online persona to their actual identity.
- Illicitly putting different entities in their terms and conditions (T&C): by adding erroneous information or different businesses in their T&Cs, infringers engage in misleading activities with the intention of deceiving users and authorities about who really owns and controls the app, making it more difficult to enforce copyright protection.

## Item 27. Case example – Xtream codes

### Xtream codes case

The Xtream Codes case revolved around a well-known software platform used by IPTV providers to manage and provide streaming material to their customers. This case referred to a large legal action against the owners and users of the Xtream Codes IPTV platform.

In a coordinated operation against Xtream Codes in September 2019, officials from Bulgaria, France and Italy shut down the platform and detained its operators. As they had enabled IPTV providers to illegitimately broadcast copyrighted content, such as TV channels, movies, and sporting events, the authorities charged Xtream Codes with promoting copyright infringement.

The Xtream Codes legal dispute brought to light the expanding initiatives taken by law enforcement organisations and copyright holders to stop copyright infringement in the digital age. Additionally, it emphasised how crucial it is to pursue legal action against websites and other services that permit and facilitate the unlawful streaming of copyrighted information. However, following an appeal, on 3 August 2021, the Court of Appeals of Naples found no evidence to show that Xtream Codes Ltd had acted illegally.

Furthermore, regarding the setup of apps that infringe copyright-protected digital content, when an app is not visibly harmful or threatening, the apps tend to be user-friendly, enticing users to continue using them. By using more of the abovementioned tools, developers can produce intuitively usable and more specialised apps that offer features found in various other apps. The following are five types of apps, that fall within the scope of this study, which may be used to facilitate IP-infringement.

- **MP3 download apps:** these types of apps are often linked to music, or other audio, content, and allow users to download MP3 files directly to their devices. They are usually sourced from a domain and downloaded directly from this domain. While some of these apps may be used to download open-sourced music, their functionalities may be misused to also download copyrighted content.
- **Stream ripping apps:** apps that allow users to download permanent copies of the audio (or audio-visual) file from content available on a licensed streaming app, without authorisation. They may be initiated by the following steps: first, the URL of the desired content is copied and pasted into the converting app. The user then chooses the format in which they desire the content and downloads it for use. On the website of one of these suspected infringing apps, they advertise themselves as an 'All-in-one Music Downloader' covering more than 1 000 websites from which music can be downloaded, such as Spotify, YouTube, SoundCloud, Vevo and Facebook. The general look of these MP3 apps is simple in design: a tab showing content downloaded and a tab for converting files from various types of media to MP3 <sup>(60)</sup>.
- **Embedded MP3 apps:** these are apps containing MP3 files embedded within the APK file of the app itself, rather than directing users somewhere else to download the file. These apps are easily identifiable as they generally have file sizes of more than 50MB

<sup>60</sup> Van der Sar, Ernesto, RIAA Ramps up Efforts to Remove Music Download Apps from Google Play, accessed on 10 October 2023.

and can be dedicated to music from a single artist. In this case, a hypothetical example would be an app claiming to be a music player that offers a vast collection of songs for users to listen to offline.

- Parasitic apps: apps that tend to source content from platforms such as YouTube, often disguising the source of the content and often having the appearance of a music streaming service like Spotify. They normally obtain the content by way of a link to a free service like YouTube; in doing so they breach the terms and conditions (T&C) of YouTube, by offering services that these platforms do not, such as offline listening, downloads, and removal of advertisements. Apps found in this category that are suspected of IP infringement are easily accessible on alternative app stores. They advertise themselves as ‘tweaked versions of the original music app created and developed as free and open-source apps’. Usually, they offer ad-free music and offline downloads without having to pay any premium subscription, and their logos resemble elements of the well-known apps in order to confuse the user.
- Unauthorised streaming apps: these can often circumvent technical protection measures applied by licensed streaming services; they hack these protections to allow users to stream content from these platforms. An example would be an unauthorised streaming app that directly hosts their own servers or obtains content from other infringing sites, circumventing technical security measures <sup>(61)</sup>.

### III.B Key enablers: gateways



This section focuses on the key enablers of IP crime that distinguishes IP crime enabled by apps from IP crime not involving apps, namely the gateway from where the app can be accessed and downloaded to the device in question.

IP criminals involved in illegal sharing of copyright-protected digital content and other copyright related crimes are usually focused on the gateway or channel through which they can disseminate content.

From an enforcement and investigative perspective, the gateway will usually be of unique importance. App stores and app marketplaces might have in place precautionary, preventive, and proactive measures to avoid apps enabling IP crime, and there will often be different types of evidence available from the gateway, including basic subscriber information, transactional data, involved IP addresses, correspondence, and payment information. Read more about internet investigation in V.C.2.b, and digital evidence in VI.A.1.

---

<sup>61</sup> Showbox app (2023), “[Showbox - Best Free App for Streaming Movies and TV Shows](#)”, accessed on 30 April 2023.

### *III.B.1 App stores, app marketplaces and other app brokers*

App stores, marketplaces and other app brokers are fundamental to the market value of the app industry, enabling creators and entrepreneurs to disseminate their apps to users. App stores are popular gateways for apps, but in their same function, app users have the option to obtain their apps from app marketplaces or other app brokers.

There are a number of various types of entities that broker the connection between the app developer and the app user, and while the precise definition of each of these entities and distinction between them might be unclear, they are all characterised by roles as key intermediaries in the app ecosystem.

The gateways through which apps are distributed may encompass official app stores, including stores from major hardware platforms (e.g., smartphone, TVs, or video game consoles) or operating systems (OS), such as those that provide their own app stores on their devices. These official app stores are often embedded within the OS of the devices.

Alternative app marketplaces and open app stores are additional gateways where internet users can directly download and integrate apps within their operating systems, usually directly from the website of the alternative app marketplace developer <sup>(62)</sup>.

Alternative app marketplaces can also be downloaded and used in addition to app stores although they may not be managed by the same reviews boards as those of app stores.

Third-party app stores are also alternative marketplaces used for downloading and sharing mobile apps that are not associated with major device manufacturers. Third-party app stores can be developed by the big technology companies, while others may be developed by smaller companies within the app ecosystem. Some major technology companies have begun facilitating the integration of third-party app stores within their devices and app stores <sup>(63)</sup>.

Suspected infringing apps can make their way into any of these gateways. To avoid this, the gateways put in place various precautionary, preventive, and proactive measures. The related policies and processes differ for each of these gateways. Ultimately, each 'gateway' establishes their own standards to govern their app ecosystem, in an attempt to create a secure and safe environment for users <sup>(64)</sup>.

---

<sup>62</sup> Apple Support (2024), '[About alternative app marketplaces in the European Union](#)', accessed on 18 March 2024.

<sup>63</sup> Holt, Kris (2024), '[iOS 17.4 is here, enabling third-party app stores in the EU](#)', accessed on 20 March 2024.

<sup>64</sup> The Observatory has published a paper, complementary to this study, on 'Apps and App Stores', which discusses the DSA, and the consideration of online marketplaces and app stores, in greater detail.

Item 28. **Enforcement and investigative measure – cooperation with app stores**

**Enforcement and investigative measure:  
cooperation with app developers and app stores**



The content of this report is complementary to the research led by the Observatory through the Cooperation with Intermediaries Expert Group on the misuse of Apps and App stores, focusing on how this ecosystem can be misused for intellectual property infringing activities, and how these misuses can be counteracted through good practices. A discussion paper on the topic will be published in parallel with this report <sup>(65)</sup>.

The discussion paper covers various good practices including:

- preventive measures related to app stores developer agreements and policies;
- preventive measures related to app stores know your business customer (KYBC) and user profile verification;
- preventive measures related to review processes;
- reactive measures related to notice and action mechanisms;
- reactive measures related to automate alerts to users;
- reactive measures related to cooperation initiatives with the advertising sector and law enforcement authorities.

It should be noted that the drafting of the discussion paper took place before the full application of the Digital Service Act (DSA) and the Digital Markets Act (DMA <sup>(66)</sup>). In that respect, the Observatory and its experts worked on the understanding that some of current functioning of the App Stores and the good practices identified in the discussion paper would turn into regulatory obligations or will need to be adapted in order to ensure compliance with the DSA and DMA. Experts agreed that it would still be timely to analyse such good practices, while simply mentioning which specific provisions of the DSA may affect them.

IP criminals have an interest in bypassing precautionary, preventive, and proactive measures, for example by way of direct downloads and downloads from other sources (see III.B) <sup>(67)</sup>. A recent study found that IP criminals try to adopt new techniques, like versioning (see IV.A.3), to get illegal apps through the security scans of app stores and app marketplaces <sup>(68)</sup>.

### *III.B.2 Direct downloads and unauthorised downloads*

Direct downloads of apps can happen directly from the app developer, or a dedicated website related to the app itself.

The security and preventive measures in app stores and marketplaces to prevent their users from downloading apps facilitating IP crime might not be present when an app can be directly downloaded.

<sup>65</sup> More on this in the [Observatory's discussion paper on Apps and App Stores](#).

<sup>66</sup> The [Digital Services Act \(DSA\)](#) (2022/2065) and the [Digital Markets Act \(DMA\)](#) (2022/1925).

<sup>67</sup> Davis, Wes (2024), [A sneaky piracy app is trending in Apple's App Store](#), accessed on 15 February 2024.

<sup>68</sup> Alan Friedman, Phone Arena (2023), [Malware was downloaded over 600 million times in 2023 from the Google Play Store](#), accessed on 15 February 2024.

Downloading from unauthorised sources can happen in many different ways, often by way of bypassing legal, licensing, technical or geographical restrictions enacted by app developers, app proprietors, gateways, platforms, or any other part of the app ecosystem.

### III.C Execution and value capture



IP criminals continue to find new ways of infringing copyright-protected digital content and offering services that appears attractive and competitive to ordinary internet users. While such developments seem to be more evolutionary than revolutionary, it is clear that IP criminals are highly adaptive to user needs and preferences while making enforcement and investigations as difficult as possible.

A recent case led by the Spanish National Police, with the support of Europol and law enforcement authorities from Andorra and Portugal, is an example of how specialised these criminals have become. An investigation began in October 2018 to dismantle a criminal group that was distributing illegal video streams. The Spanish police received several complaint reports from the Alliance for Creativity and Entertainment, Football Association Pretoria, the Premier League, and the Spanish Football League (La Liga Española de Fútbol) about an app that was illegally distributing video streams, which had been downloaded by more than 100 million users through various websites. The investigation uncovered several linked websites and platforms based in Spain and Portugal but with servers in Czechia. The Spanish business that was engaged in the illegal activity made money from advertisements. They were able to sell user information to a business involved in botnet and DDoS attacks thanks to their computer infrastructure and processing power. The total illegal profits, according to the investigators, exceeded EUR 5 million<sup>(69)</sup>.

Depending on how the app is being used and the type of infringement, apps can record and profit from IP infringement in a variety of ways.

#### III.C.1 Use

The landscape of copyright-protected digital content consumption has changed over the years. The user experience has evolved significantly, even sometimes mimicking the functionalities of legitimate apps. Apps for the infringement of copyright-protected digital content will usually be installed by internet users on their private devices and for purely private reasons. Devices used for business or professional purposes are often subject to company security and 'bring your own device' policies to avoid security risks. As such, third party apps are very difficult, if not impossible, to install on business devices. Therefore, these apps are generally focused on the end user, making the business model ultimately business to consumer (B2C).

---

<sup>69</sup> EUROPOL / IPC3 / EUIPO (2021), [Illegal mobile application with more than 100 million users taken down in Spain](#).



Apps that mimic functionality are known as clone apps and are characterised by the imitation of the legitimate app's graphical design features. In an effort to profit from the legitimate app's popularity, IP criminals will use these features with an altered functionality that caters to their infringing business model.

### *III.C.2 IP crime*

The infringement of copyright-protected digital content such as music, films, software, or e-books is a major IP crime threat and entails disseminating such content online without authorisation from the copyright holder, thus causing substantial financial losses to the industry and economy as a whole.

Stream ripping software can aid in facilitating online copyright infringement and is available in app form and on some app stores, posing a major concern for copyright holders. In using this software or app, users are able to create a permanent downloadable copy of a sound recording from a licenced streaming service. Essentially, users must normally search for particular content, for example on media sharing platforms, and then, after having been provided with the URL, the app will allow the user to download and convert the audio track of a music video or any other video including music to an MP3 file format. A real-life example is the FLVTO YouTube downloader, which is one of the largest YouTube-to-MP3 converters in the world. It allows users to paste the link of a YouTube video and convert it to an MP3 file for free, infringing IP.

In August 2021, the site was blocked in the United Kingdom and the United States<sup>(70)</sup>, but it is still available in other countries as an app. The app allowed users to add videos to a playlist or to their favourites and share them with others, also displaying recently watched videos and any playlists created within the 'My Music' screen. Users are able to click through various screens showing the home page, their music, and their downloads; alternatively, when they want to explore, they can 'discover' or search for specific content.

Beyond audio-visual content, apps may also be used to facilitate access to text content, without the proper authorisation from the IP owner. In some cases, IP criminals purchase or access copyright-protected e-books or textbooks, among other text sources, and disseminate them free of charge through apps to users.

*When investigating IP crime, speed is key. Therefore, taking time can lead to more harm. On top of that, with the complexity of apps, investigators may forget about the main things they are looking for. Developing a structured investigation method keeps people focused and makes sure that all the reports generated contain the same key elements of an investigation.*

IP crime expert

---

<sup>70</sup> Paul Resnikoff, Digital Music News (2021), [FLVTO, One of the World's Largest YouTube-to-MP3 Converters, Officially Shuts Down In the US & UK](#), accessed on 14 February 2023.

Item 29. **Enforcement and investigative measure – MICE framework**

**Enforcement and investigative measure: MICE framework**



Coordination within the industry itself, in collaboration with law enforcement, can help to prevent IP infringement. There is no fixed structure on investigating into IP criminals, which may make it difficult for law enforcement to understand the specifications of each case. Several businesses that focus on combatting IP infringements have developed cohesive procedures to tackle this issue. For example, Universal Music Group have elaborated a framework to structure the process of normal investigations, calling it the MICE framework (money, infrastructure, content, and exposure).

**Money:** this element focuses on the methodology through which IP criminals generate revenue, whether advertising, subscriptions, and fraud. With these types of IP criminals, 'follow the money' protocols can be applied to find out what is happening, where the money comes from, where it goes, and who the beneficiary is.



**Infrastructure:** the second element examines how the infringing-content reaches the user and who is enabling the correct 'technical' distribution. The focus is on where the content is hosted (front- or backend), the domain names used, nameservers, third-party APIs, registrars, and registries, and the operators.

**Content:** the third element highlights the type of infringing content shared to users, such as copyrighted material, and how the IP criminals are accessing that content to deliver it. There is also focus on the update frequency of the material.



**Exposure:** the final element analyses how the infringer promotes their app and where the users can search for it. In the case of app promotion, IP criminals can use the same channels as legitimate businesses, through social media advertising and other channels. Along with the promotion of the app, IP criminals tend to say where the app is available.

The challenge with apps is that there are many directions in which the investigation can go, potentially distracting investigators from the case's key elements. Therefore, the MICE diagram keeps businesses and IP owners focused on making sure that all investigative reports consider these four key elements that ultimately highlight the fundamentals of the investigation: the who, what, when, why, how, and where.

III.C.3 *Criminal gain*

III.C.3.a **Revenue generation**

In terms of revenue, IP criminals can pursue criminal gain through several methods, some of which may overlap with business model 3 on IP infringement for fraudulent and malicious purposes (see V). A common revenue source is digital display advertisements revenue from IPTV streaming platforms.

- Advertising revenue: IP criminals may generate revenue through advertising, requiring advertisers to pay to display their content to users. When an app infringes IP, the app developer may profit from displaying advertisements alongside the infringing content. This model can take various forms, such as intrusive pop-up advertisements or deceptive practices, contributing to the IP criminals' financial gain.

- In-app purchases: some apps may offer physical or virtual goods for sale through their app as well as the option to purchase extra features for the app, prompting users to make additional purchases while using the app. In-app purchases are usually optional and commonly seen in gaming apps, where players may be enticed to make in-app purchases to level themselves up or gain a gaming advantage.

Many apps in this category use advertisement pop-ups. The apps usually allow users to watch copyrighted-protected digital content<sup>(71)</sup>; while users are browsing and streaming material, the app displays a variety of advertisements. Moreover, they often require a subscription to use or require payment to access premium features or content.

- Subscription revenue: apps that require users to pay a regular fee to use. When requiring subscriptions, IP criminals have better control as to who they allow onto their platforms. This technique is used because of the challenge that law enforcement faces in tracking the funds and blocking the payments.
- Freemium model: some apps are based on a freemium model, meaning that only basic functionalities and features are available free of charge. Users must pay either a monthly subscription, or one-time fee subscription, to access premium features or additional content.

A recent initiative launched aims to enhance trust in the digital advertising industry by limiting pirate sites' access to advertising funds. The initiative aims to defund pirate sites and protect advertisers from negative associations by ultimately developing a blocklist that combines pirate site data with information from anti-malware vendors to also target the issue of malvertising (see V.C.2.e on deceptive advertising techniques in apps)<sup>(72)</sup>.

A study showed that downloaded audiovisual piracy apps may carry a higher chance of being embedded with malware, if coming from untrustworthy sources<sup>(73)</sup>. IP criminals intending to distribute malware and potentially unwanted programs (PUPs) to users are able to do so by bypassing the measures put in place by the various gateways and thus harm internet users<sup>(74)</sup>.

*In terms of how pirated copyright protected content is consumed, both the landscape and revenue models have changed with app piracy. Criminals are not interested in giving everyone access to their platform, they only allow the people that they want – through subscription mechanisms – making it a more controlled space.*

IP crime expert

<sup>71</sup> DZAPK (n.d.), [MegaBox HD](#), accessed on 20 June 2023.

<sup>72</sup> Maxwell, Andy (2024), '[Pirate Sites with Malicious Ads Face Restrictions Under New Initiative](#)', accessed on 19 March 2024.

<sup>73</sup> '[Study On Malware And Audiovisual Piracy Highlights Significant Risks To European Consumers](#)', 2022. Retrieved from Anti-Piracy Alliance (AAPA), accessed on 27 February 2024.

<sup>74</sup> EUIPO (2018), '[Identification and Analysis of Malware on Selected Suspected Copyright-Infringing Websites](#)'.

In terms of IPTV crime, the ecosystem normally involves both B2B and B2C sales of television signals<sup>(75)</sup>. IP criminals do not expose themselves directly to the internet: they can sell their codes through panels, such as the Xstream Codes panel (see III.A.3). Although the Xstream Codes panel served as a management platform for IPTV service providers and was not intended for the purpose of sharing app codes, developers would nonetheless use it to share codes or access credentials related to IPTV apps. To authenticate users and enable them to access IPTV services, developers would integrate their IPTV apps with the Xstream Codes panel. As part of this integration, the panel would generate special credentials or access codes that were given to users by the service providers. Usually, users would enter these codes to access the IPTV app and the content offered by the provider. Although this is not a source, it still exists and is used by IP criminals and resellers who provide access to infringing content.

To avoid detection, IP criminals have created new and innovative ways to charge their users. In some cases, to hide where the money is going, an app may inform the user when making the payment that the charge for their services will appear on the user's bank statement under another name, so as not to be detected by law enforcement.

### Item 30. Important emerging trend – digital display advertising

#### Important emerging trend: digital display advertising



Digital display advertisements are numerous across digital services, especially in apps, as they play a significant role for both developers and users. For developers, the implementation of advertisements is usually driven by revenue generation and maintaining the interest of advertisers to ensure future revenue generation. For users, advertisements can cater to user tastes and preferences, enhancing the user experience.

Some app developers have established a way to circumvent any potential loss of user engagement, while still maintaining sufficient advertising revenue streams, through invisible ads. Such apps will load advertisements while the device's screen is off; this appears to benefit the user, by not bombarding them with ads, and the developer, by reporting high KPIs in displaying the ads. However, in reality, users are subject to a number of risks: battery drainage, unauthorised data consumption, potential information leaks, and the 'disruption of user profiling caused by Clicker behaviour'<sup>(76)</sup>. For advertisers, it is a form of fraud against those who unknowingly pay for invisible advertisements, thinking that they will be visible.

Moreover, when coupled with malvertising and fraud, digital display advertising can deceive users into believing in the legitimacy of a product or service, more so when the advertisements are displayed on traditional websites, social media or apps that redirect users to the source of the fraudulent offering (see V.C.2.e on deceptive advertising techniques in apps). These practices typically use high discount offers to attract consumers.

<sup>75</sup> Read more about the trends within the ecosystem of IPTV crime in the EUIPO's Discussion Paper on [Live Event Piracy](#) (2023), where both B2B models and B2C models are discussed. For more information on the infringing business model of IPTV, see Phase 3 of the Research on Online Business Models Infringing IP Rights, titled [Illegal IPTV in the European Union](#) (2019).

<sup>76</sup> McAfee Labs (2023), [Invisible Adware: Unveiling Ad Fraud Targeting Android Users](#).

### III.C.3.b Money laundering

IP criminals have several ways to generate gain through apps. Money laundering is a relatively standard activity for illicitly generating revenue; in more modern times, money laundering can now be facilitated by cryptocurrencies.

Cryptocurrencies often offer a degree of anonymity or semi-anonymity and can be traded on decentralised platforms, where

cryptocurrencies can be exchanged for other cryptocurrencies, as well as exchanges, where cryptocurrencies can be exchanged for fiat currencies. This makes them an attractive tool for money laundering. Transactions made with cryptocurrencies can sometimes be difficult to trace to an individual due to the pseudonymous nature of digital wallets and the lack of a central authority monitoring the exchanges. The ability to quickly move funds across borders further perpetuates the layers and integration stages of money laundering.

There are various types of cryptocurrency technologies that may be misused for money-laundering purposes, such as privacy coins and crypto mixers. Privacy coins are untraceable by design, offering a higher level of anonymous blockchain transactions, for instance, by withholding details about the balance and source of origin of the coins from third parties. Crypto mixers are a technology that can blend potentially identifiable cryptocurrencies for the purpose of obscuring the source of origin, making them untraceable. Cryptocurrencies from multiple sources are sent to one address (the mixer) and blended together, after which they are split into several portions and sent to different addresses. The process may be repeated a number of times before the cryptocurrency reaches a final destination<sup>(77)</sup>.

*There is a jurisdictional challenge during investigations when trying to find out who is behind an app. It is often complicated to investigate who the developer or proprietor of an app might be because they use fake information, a nickname, or fake ID, or use different technologies to obfuscate their location.*

IP crime expert

---

<sup>77</sup> United Nations, "[Money laundering through cryptocurrencies](#)", accessed on 29 February 2024.

Item 31. **Enforcement and investigative measure – cryptocurrency forensics**

**Enforcement and investigative measure:  
cryptocurrency forensics**



Cryptocurrency forensics refers to the application of tools and techniques to track and analyse transactions involving cryptocurrencies such as Bitcoin and Ethereum, which are increasingly used for all types of financial transactions, whether legal or illegal. Some cryptocurrency forensics tools are freely available as open-source or proprietary software.

The main objective of cryptocurrency forensics is identifying the owner of a cryptocurrency wallet that has been involved in a transaction under investigation. By establishing the ownership, an important step towards attributing a cryptocurrency payment to an individual suspect is taken.

One way of achieving this attribution is to keep following the payment trail until it reaches a financial institution, such as a cryptocurrency exchange or other financial institution, that keeps reliable know-your-customer (KYC) information.

Cryptocurrency forensics involves a combination of internet investigation of publicly available information about cryptocurrency transactions and information stored offline.

A successful cryptocurrency investigation will therefore usually require:

- a certain level of understanding of blockchain cryptography, the underlying technology behind cryptocurrencies;
- access to and understanding of the functionalities of cryptocurrency forensics tools;
- a legal measure to require an involved intermediary to disclose relevant information.

One example of an app impersonating a legitimate business was a suspected IP-infringing app based in Norway. It was available in app stores and as a Chrome extension and offered blockchain-based compensation for creators. The app connected with illegal sources to access content for a small fee of EUR 2, which would go to the relevant party or stakeholder. This approach displayed innovative characteristics, and if applied within the legal framework, could hold potential for legitimate apps, with smart contracts ‘regulating’ this aspect; however, in the case of the Norwegian app, most of the money made stayed within the company.

### III.C.3.c P2P filesharing

In terms of illegal IPTV, subscription-based apps, are commonly used in IP crime, in addition to the lesser used traditional BitTorrent and P2P filesharing systems. The BitTorrent protocol entails sharing large files in a peer-to-peer network. It requires at least one user (a peer) to make content available, which can then be downloaded and further shared by other users; while this is not necessarily an illegal practice, the method is commonly used to download copyrighted material<sup>(78)</sup>.

<sup>78</sup> Bram Cohen (2008), [The BitTorrent Protocol Specification](#), accessed on 11 February 2023.

A well-known case was that of the Popcorn Time application, a free open-source app, available on different platforms, that used a BitTorrent client to stream videos without a licence – ultimately an illegal alternative to legitimate streaming services. Popcorn Time was a P2P-based system that presented itself as an easy-to-use app allowing users to search and stream a large selection of films and TV shows without the need to register or subscribe.

The case was considered by the Supreme Court of Denmark, specifically in relation to the defendant's guidance on how to use the Popcorn Time streaming service and their supplying users with links to websites where the app could be downloaded. In doing so, the Supreme Court found that the defendant had intentionally committed copyright infringement contributory to the acts of the app's operators and of its users and must have realised that the website's instructions would lead to copyright infringement of protected digital content. The defendant obtained around EUR 700 000 euros in advertising revenue from operating the website <sup>(79)</sup>.

The following is a detailed description of the case itself.

### Item 32. Case example – Popcorn time application

#### Popcorn time application case

The Popcorn time app was relatively popular, as it allowed users to easily access copyright-protected digital content without going through the necessary permissions and consent of the IP owners. Each film or TV show included the original poster art, the year of release and, when clicked, a short description of the content itself. Users could see content in real time while also sharing it with others using the BitTorrent protocol, effectively turning them into both consumers and distributors of copyrighted content.

The service was declared illegal in August 2015 by the United States District Court of Oregon – Portland Division in *Cobbler Nevada, LCC v Anonymous Users of Popcorn Time*, in which the District Court affirmed that Popcorn Time existed only for the purpose of stealing copyrighted material <sup>(80)</sup>. The Danish Supreme Court also found in 2020 that the platform had knowingly contributed to IP infringements <sup>(81)</sup>. Several other countries also blocked all access to the official downloads of Popcorn Time, such as the United Kingdom, where in April 2015 the UK High Court issued an order requiring operators Sky, TalkTalk, Virgin, BT, and EE to block access to five Popcorn Time forks, arguing that it was a platform used exclusively to view copyright-infringing content <sup>(82)</sup>.

This app was therefore the target of multiple legal challenges from both IP owners and other players in the entertainment industry because of its widespread popularity among users and blatant infringement of copyright laws. The app's creators remained anonymous, which posed even more challenges for IP owners in identifying the parties responsible for the app's development and upkeep. Both individual users and software developers were the targets of lawsuits seeking redress for copyright infringement; despite these legal proceedings, numerous variants and branches of Popcorn Time persisted, exacerbating the challenges for IP owners and general enforcement.

<sup>79</sup> Find more information on the Danish Supreme Court website: <https://domstol.dk/hoejesteret/aktuelt/2020/1/om-medvirken-til-ulovlig-streaming/#popcorn>.

<sup>80</sup> Govrinfo (n.d.), *15-1550 - Cobbler Nevada, LLC v. Anonymous Users of Popcorn Time*, accessed on 11 February 2023.

<sup>81</sup> Lundgrens (2023), *The Supreme Court of Denmark reaches decision in the 'Popcorn Time' case*, accessed on 18 October, 2023.

<sup>82</sup> eIEconomista.es (2015), *UK blocks multiple pages distributing Popcorn Time*, accessed on 11 February 2023.

### III.C.3.d Generic media players

Among apps that are not intentionally developed to infringe, but the functionality, configuration or modification of which in some way allows IP infringement, generic media players pose a very pressing threat to IP owners. These media players are software programs installed on or hardware devices that are capable of playing media files<sup>(83)</sup>.

The main functionality of a generic media player is to allow streaming or local/external content playback using for example M3U file. An M3U file is an audio playlist file and an abbreviation of 'MP3 URL'. A media player can queue up audio, and occasionally video files, for playback using an M3U file as a pointer to those files<sup>(84)</sup>. There is a distinction between these media players, some of which function as completely legitimate software that merely provides media, with no intent to infringe, and other software provider platforms that intentionally share illegal content and infringe IP. The issue is that even the legitimate media players' configurations can be used to access illegal content streaming, posing a challenge for the industry in trying to prove that some software platforms are only developed for the purpose of sharing illegal content. It is important to highlight that these generic media player apps are legitimate and legal; the problem is that they are misused by infringers.

The source code of such services can be free and open source. In particular, one app is a portable, cross-platform media player and streaming media service that allows users to add plugins and extensions to improve the user experience<sup>(85)</sup>. Third-party developers have created add-ons and plugins for users to access copyrighted material, such as premium TV channels, without the IP owners' permission. These services have been blocked in some countries but are still available in a number of others. The interface often resembles the built-in PC file explorer, displaying the content on the device, the devices connected, the devices on the local network, and programs on the internet. Users will usually be able to see their downloaded content and watch or listen with ease.

Similarly, another free, legitimate, and open-source media player has been used for the same illegitimate purposes. This app was created by a non-profit technology consortium and is available for multiple operating systems and hardware platforms, allowing users to play and view most videos and music.<sup>(86)</sup> As with most similar platforms, third-party developers have created add-ons and plugins allowing users to access copyrighted material without the IP owners' permission. These add-ons are promoted through legitimate social media apps or encrypted instant messaging and voice over

*With new social media platforms, IP criminals can apply language that direct users to illegal content provided by apps without attracting the attention of law enforcement. A new focus is influencers who are paid to advertise IP-infringing apps on social media.*

IP crime expert

<sup>83</sup> Computer Hope, [Media Player](#), accessed on 11 February 2023.

<sup>84</sup> Tim Fisher (2021). [M3U File \(What It Is & How to Open One\)](#), accessed on 12 February 2023.

<sup>85</sup> Softwers Downloading. [VLC Media Player Free Download](#), accessed on 12 February 2023.


<sup>86</sup> [Kodi](#) (2023), accessed on 12 February 2023.



internet protocol (VoIP) apps, where users even explain how to download them and access the illegal content.

Item 33. **Important emerging trend – social media and encrypted instant messaging apps**

**Important emerging trend:  
social media and encrypted instant messaging apps**



Social media and encrypted instant messaging and voice over internet protocol (VoIP) apps have the primary function of facilitating communication between users. While such services are out of the scope of this report, both technologies may be misused by IP infringers as effective and safe communications tools for public, private, or select-group communication. To some extent, encrypted instant messaging and VoIP apps can provide alternatives to communication via the dark web (see III.A.2) as they have the capacity to provide a layer of obfuscation of the content of the communication and for some specific services provides opportunities to hide the identity of IP criminals. Compared to the dark web, instant messaging apps might be attractive alternatives due to the higher number of users, enhanced user friendliness, and general high latency and low levels of downtime.

Social media and encrypted instant messaging services can also be used for promotion of illegal apps infringing IP or facilitating other serious crimes, and special techniques like hidden links and live marketing can be applied. They can thus aid in disseminating copyright-protected digital content, marketing and distributing IP-infringing goods, carrying out fraudulent activities, and stealing trade secrets.

Some specific encrypted instant messaging services or devices has become strategic parts of organised criminal groups day-to-day operations<sup>(87)</sup>.

Many other media players have a similar functionality, with the only difference being that they have been deemed illegitimate apps.

There are many more apps that can infringe copyright-protected digital content. Some of these apps even provide links that can be opened in an external app, such as Arena4Viewer, which displays live sports events and games. There are websites available with detailed instructions on how to download the app, including screenshots<sup>(88)</sup>.

### III.C.3.e **Infringing media players**

Just as legal generic media players can be misused by criminals to commit IP crimes, they have created infringing media players of their own. The difference is that generic media players are created with the legitimate purpose of letting anyone stream, playing back their home content, or using an M3U and opening it in their generic media player to consume their desired content. Infringing media players, on the other hand, are created with the sole purpose of distributing content illegally.

<sup>87</sup> Europol (2024), [Decoding the EU's most threatening criminal networks](#), accessed on 7 May 2024.

<sup>88</sup> Patrick (2023), [How to Install Arena4Viewer on FireStick for Live Sports](#), accessed on 5 July 2023.

There are vast numbers of open-source video streaming apps used for infringement purposes; one large player, Mobdro, was a third-party app unavailable on conventional app stores due to copyright infringements. Users therefore sought unofficial sources, like alternative app stores, from which to download the file. The below is a detailed description of the Mobdro application and case.

#### Item 34. Case example - Mobdro

### Mobdro case

With the help of the well-known streaming app Mobdro, users could access a variety of TV shows, films, and sporting events without the required permission from the copyright holders. Using IPTV technology, the app was able to stream live and on-demand material online.

As the app allowed users to see copyrighted content without paying the proper owners or acquiring the relevant permissions, Mobdro's involvement in copyright infringement drew the attention of copyright holders and stakeholders in the entertainment sector.

To fight against infringement of copyright-protected digital content, law enforcement agencies and copyright owners filed lawsuits against Mobdro and its owners. Many law enforcement agencies in various jurisdictions pursued criminal and civil actions against individuals responsible for the creation, dissemination, and use of the app.

The Mobdro app legal dispute brought attention to the expanding initiatives to enforce IP in the app ecosystem and solve the problems caused by unlicensed streaming services. Additionally, it increased knowledge of the legal consequences that app makers and users who infringe IP through such platforms could face in court.

The effectiveness of this app was significantly influenced by content delivery networks (CDNs). This is also the case for other providers of illicit content. A content delivery network (CDN) is a collection of servers dispersed over numerous locations with the goal of disseminating material such as videos and photos to users more effectively and quickly. Mobdro used a CDN to provide requested content from the server closest to the user's location whenever a user requested a video stream or other content. This decreased latency and enhanced the streaming experience as a whole<sup>(89)</sup>.

Digital content is protected against unauthorised use and disseminated using technical protection measures (TPM). Only authorised users can access the information because of encryption and licensing controls. TPM prohibits users from downloading or redistributing copyrighted information, in the context of streaming videos, without the required authorisation<sup>(90)</sup>. While legal streaming platforms may use TPM to safeguard copyrighted content, infringing apps such as Mobdro typically work around TPM and provide unlawful access to copyrighted content.

The platforms of these video streaming apps are often user-friendly and resemble a catalogue displaying the various categories of media available, from TV shows to films and sports,

<sup>89</sup> Helen Vakhnenko (2023), [Content may not be copied, reproduced, distributed, displayed, downloaded or otherwise used for any purpose without the prior written consent of owners](#), accessed on 13 June 2023.

<sup>90</sup> Fortinet (n.d.), [Digital Rights Management \(DRM\)](#), accessed on 13 June 2023.

among others. When a category is selected, users are taken to a list of links to choose from and begin their viewing.

Item 35. **Law enforcement investigative strategies relevant to infringement of copyright-protected digital content**

## Law enforcement investigative strategies relevant to infringing business model 1

When law enforcement authorities are investigating an app that is suspected of facilitating the infringement of copyright-protected digital content, there are at least five strategies that may be implemented as part of the investigation.



The **follow the stream** strategy entails investigating networks involved in the infringement of copyright-protected digital content and finding the network of resellers connected to a wholesaler of IPTV streams. Doing so requires tracing the actual audiovisual content from the consumer to its source, which can be very difficult given the labyrinth-like ecosystem that interconnects all streaming apps, both illegal and legal.

The **follow the pattern** strategy may connect individual occurrences of trade secret theft facilitated by apps to larger IP crime operations. In this strategy, clusters of IP crime can lead to the discovery of the full scope of the operation. In some cases, an infringing app's operation may seem isolated from other operations, but investigating the infrastructure, ownership and money flow of the operation may reveal connections between several apps. Some investigative techniques used in this strategy include, but are not limited to, the use of internet investigations (e.g., open-source intelligence (OSINT), and obtaining data from internet intermediaries).



The **follow the money** strategy involves identifying the infrastructure related to money inflow, identifying the persons involved, and disrupting the money flow. Doing so will also require an understanding of the tools used to obtain money, whether through electronic, cryptocurrency or traditional bank mechanisms. Following the money may also entail retrieving evidence related to payments and supporting future money-laundering charges.

The **follow the pixel** strategy includes looking for digital display advertising and electronic artefacts and identifying payments related to both. The investigation extends to all online advertising-related technologies; since many apps are largely advertising-supported, revenue may be derived from such advertising (see III.C.3.a), among other sources (see VII). When combined with the 'follow the money' strategy, the 'follow the pixel' strategy becomes very effective.



The **follow the person** strategy focuses on identifying the various IP criminals, their affiliations, and how they cooperate and collaborate as an organised crime group. Beyond individuals, this strategy also identifies limited-liability companies, foundations or associations used by IP criminals to facilitate their operation and observes the movement of targeted persons to uncover the locations in the supply chain.

Read more about business models related to infringement of copyright-protected digital content in other reports in the infringing business model series <sup>(91)</sup>.

<sup>91</sup> In the [IBM phase 5](#) report chapter 6, there is a description and analyses of access to and dissemination of copyright-infringing materials. The phase [IBM phase 3](#) report specifically analysed IPTV crime.

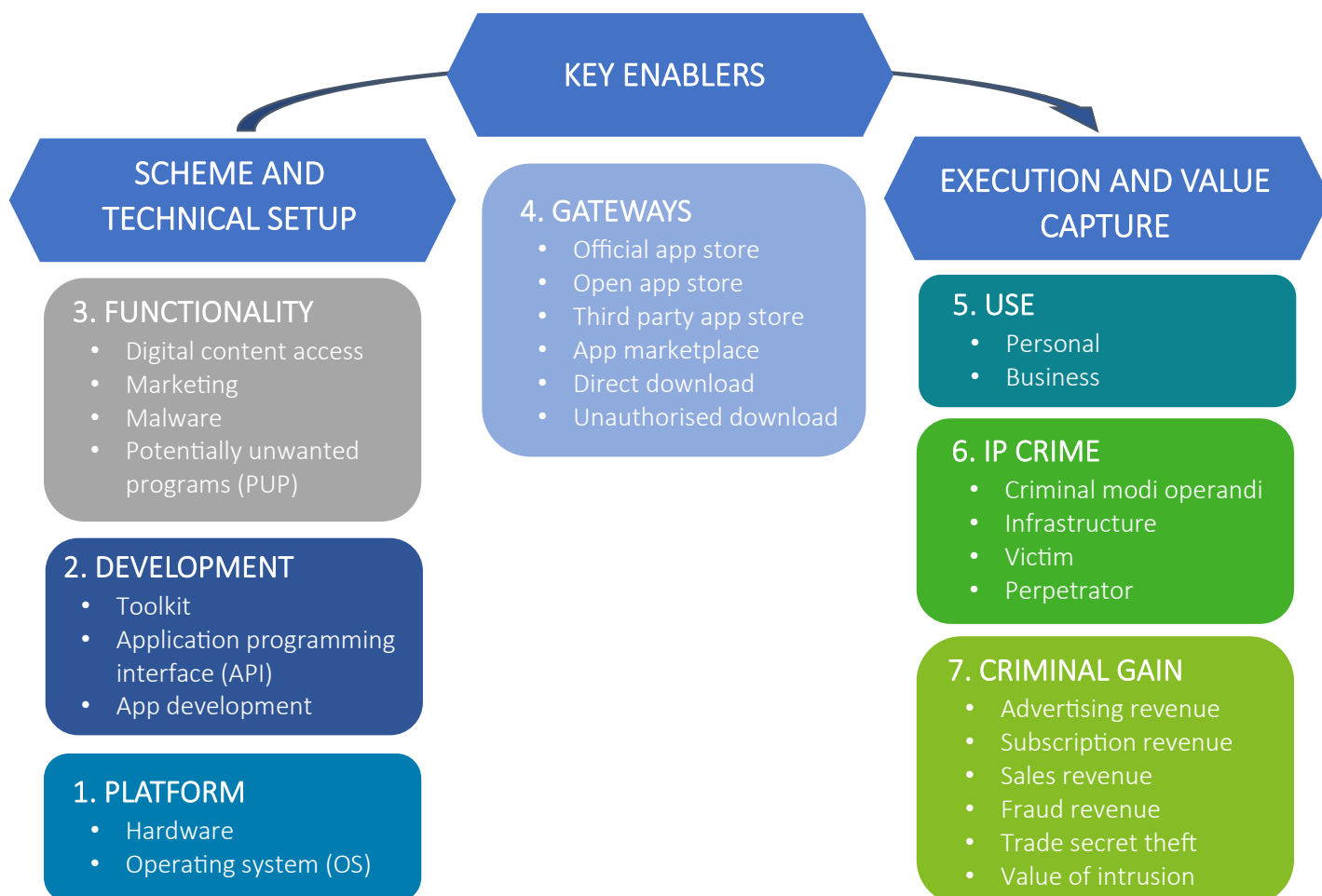
## IV Infringing business model 2: marketing of IP-infringing physical goods



While more prevalent on other online sources (e.g., e-commerce marketplaces, dedicated websites with e-shops, dark web (see III.A.2), social media and encrypted instant messaging and voice over internet protocol (VoIP) apps (see III.C.3.d)), IP-infringing physical products are also marketed through dedicated apps.

The description of the business models follows the content of *the arc of IP crime related to apps*. The business models described in relation to marketing of IP-infringing physical goods has some overlaps with business model 3 related to fraudulent and malicious IP crime (see V).

Item 36. *The arc of IP crime related to apps*



## IV.A Scheme and technical setup



IP infringements related to apps, encompass the emerging trend of marketing of IP-infringing physical goods by way of apps.

### IV.A.1 Platform

The platform for IP infringement through marketing of physical goods is the same type of hardware, hardware setup, and operating system (OS) as described in the chapter on infringement of copyright protection digital content (see III.A.1).

### IV.A.2 Development

The development of IP-infringing apps related to marketing of physical goods is to wide extent done in the same way as described in the chapter on infringement of copyright protection digital content (see III.A.2). As such, given that the current structure of technology allows for apps to respond to changing user behaviour, the means of offering counterfeit goods are broadening.

*App developers sometimes might advertise themselves, their project and tutorials by sharing their LinkedIn profiles or explaining what they do on their own Discord platforms or traditional social media profiles. This makes it easier to locate and identify them. It is harder when there is a group of people involved, but open-source intelligence (OSINT) or social media intelligence (SOCMINT) are great tools to identify the developers of these applications.*

IP crime expert

### IV.A.3 Functionality

Functionality is a growing concern, because criminals have learned that they can quickly change the functionality of their app after getting it into official app stores, without the marketplaces noticing the changes. In these cases, the functionality of an app selling IP-infringing goods very closely resembles the functionality of the legitimate app; however, once the review procedures are passed and the app becomes available for download, the function may change to better facilitate the sale of IP-infringing goods. Since no additional reviews are made after the functionality has been changed, users also remain uninformed about these changes, which result in users unknowingly infringing IP.

### Item 37. Important emerging trend – versioning

#### Important emerging trend: versioning



This trend entails developers releasing several versions of an app as an obfuscation technique. In this case, the user will encounter a completely legitimate app that is an aggregator; when it is downloaded, it will say that, to reach its full functionality, the next version of the app needs to be downloaded. In official app stores however, Usually, the next version will be found in other app stores; once the correct version is downloaded from that external marketplace, the infringing content can be accessed. Therefore, users of digital marketplaces would be unable to find the infringing app unless the updated version is installed – allowing the user to download the IP-infringing version. Usually, these apps are free and run-on advertising revenue.

A new study by the cybersecurity firm Kaspersky<sup>(92)</sup> has found that criminals have learned new techniques to get malicious apps through the security scans of app stores. The study shows that in 2023, Android users downloaded malicious apps over 600 million times through the Google Play Store. The malware was integrated after the app was introduced into the app store. The criminals would first upload a completely legitimate app to the store, and then, with an update, add the malicious features. However, doing so poses its own challenges, as official app stores may conduct reviews several times if there are changes or updates made to the app, before, during or after the app's publication<sup>(93)</sup>.

If apps use trade marks, logos, or other branding elements without permission, their marketing efforts could also contribute to IP infringement. Like any other business, IP criminals need to market their products and content to attract internet users. The way IP criminals market their goods and services through social media, encrypted instant messaging and voice over internet (VoIP) apps or other online sources is similar to typical online marketing practices.

Apps used to market IP-infringing goods pose a number of challenges:

- Misleading product descriptions: apps that facilitate the marketing of IP-infringing goods may use deceptive product descriptions or photographs to trick users into thinking they are buying authentic goods.
- Anonymous transactions: some apps support anonymous transactions or do not properly verify users' identities, when conducting a purchase or transaction. This anonymity makes it easier for vendors to sell illegally obtained goods and helps them avoid detection. Some cases of how these apps enable anonymous transactions can be through cryptocurrency payments (see V.C.3), allowing pseudonymous accounts without requiring a proper verification of the user's identity, encrypted communication channels through anonymous forums, and disposable or temporary accounts that are used to make single transactions or are active for only a short period of time.

<sup>92</sup> Alan Friedman, Phone Arena (2023), [Malware was downloaded over 600 million times in 2023 from the Google Play Store](#), accessed on 15 February 2024.

<sup>93</sup> Section 6.1 of the Apple's '[App Developer Program License Agreement](#)' accessed on 15 March 2024. More information on app store policies in the [Observatory's discussion paper on Apps and App Stores](#).

- Limited reporting mechanisms: these methods can prevent users from reporting listings of IP-infringing physical goods, allowing such products to remain on the platform.
- Social media and encrypted instant messaging and voice over internet protocol (VoIP) apps: these are tools that IP criminals can use to promote their illegal businesses. To reach a large number of users, sellers might abuse social media's capacity for public, private or select-group communication to advertise IP-infringing goods. Encrypted instant messaging and voice over internet protocol (VoIP) apps provide the possibility of obfuscation of communication and anonymity to IP criminals in marketing their infringing products. The communication aspect of both social media and these instant messaging apps, make it an ideal place for IP infringers to target clients and increase their brand popularity, resulting in the sale of more infringing products (see also III.C.3.d).
- False advertising and non-delivery: some IP criminals may use apps to falsely market goods of a seemingly high value, such as jewels or precious metals. IP criminals may also use apps to market IP-infringing goods and never deliver the goods to the customer. These examples encompass how the traditional marketing of IP-infringing goods overlaps with overt fraud against customers (see V.A.3.c).

*What we see more and more is infringing apps being advertised on social media platforms. The distribution of these apps on social media platforms that target children are a very pressing threat.*

IP crime expert

Additionally, developers of IP-infringing apps may go to the extent of advertising themselves, showing what they have created and the products they offer, which potentially makes it easier for law enforcement to locate them. They also brand their sources when they have reached a certain level of popularity in order to obtain recognition in the illicit environment, 'showing off' the highest-quality content that they offer. They also do this so that resellers will buy their content. Moreover, some logos are very generic, for example they use little white dots or letters.

## IV.B Key enablers: gateways



The key enabling gateways providing access to download an app related to marketing of physical goods are the same as described in the chapter on infringement of copyright protected digital content (see III.A.2).

From an enforcement and investigative perspective, the gateway will usually be of unique importance. App stores and app marketplaces might have in place precautionary, preventive, and proactive measures to avoid apps enabling IP crime, and there will often be different types of evidence available from the gateway, including basic subscriber information, transactional data, involved IP addresses, correspondence, and payment information. Read more about internet investigation in V.C.2.b, and electronic evidence in VI.A.1.

There are number of precautionary measures that are implemented within each gateway to prevent IP criminals enabling IP-infringement through apps (see III.B.1 on cooperation with app developers and app stores).

*While the efforts of enforcement bodies to remove apps from marketplaces are good, they do not fix the problem as a whole. Even when an app is deleted from a marketplace, it will still run on the phones where it was previously downloaded.*

IP crime expert

## IV.C Execution and value capture



IP criminals continually find or develop ways of circumventing enforcement to market IP-infringing goods, including marketing manifestly non-genuine goods and products which, to ordinary consumers, appear to be real products, but are usually offered at significantly lower prices to attract buyers.

Depending on how the app is used and the type of infringement involved, apps can generate illicit profits from IP infringement in a variety of ways.

### IV.C.1 Use

E-commerce apps that facilitate the marketing of IP-infringing goods mostly target personal use, in that they are mainly aimed at inducing consumers to purchase counterfeit or replica products and lookalikes and to access trade mark-infringing listings.

There are two types of customers in these cases, the knowing and the unknowing. A knowing customer is one who intentionally searches for these infringing goods, not wanting to purchase the original products. On the other hand, an unknowing user is one who, without their knowledge, believes that they are purchasing a product from an original shop. The unknowing user is at risk of being misled into buying a product that is not legitimate.



*The problem is that these infringing apps are very flexible, and when investigated and taken down, the criminals immediately will adapt and find new ways into attracting their customers.*

IP crime expert

Moreover, brand abuse is widespread in apps marketing IP-infringing goods: the infringing business imitates the original brand in order to deceive customers into believing they are viewing the real website or an associated page of the brand. This is also called ‘brand impersonation’. They do this by extensively replicating brand trade marks, website designs, product listings, and other elements. When a visitor arrives at the page, they are greeted by imitations of the real company’s goods and services<sup>(94)</sup>.

An example of an IP-infringing business is a malicious for-profit group, based within a major economic power and important trading partner, which created a massive network of over 42 000 web domains impersonating well-known brands and redirecting users to sites promoting adware apps, dating sites, or free giveaways. This was a massive traffic generation scheme that generated advertising revenue for the operators’ own sites<sup>(95)</sup>. The giveaways would pop up when the user entered the website and congratulated them on winning a large cash prize; the congratulations message contained instructions directing the user to a second page where they could ‘claim’ their prize, by completing a registration. To deter victims from detecting signs of fraud, the landing pages redirected visitors to a survey domain with a countdown that increased urgency to complete it. In certain cases, finishing the survey resulted in the download of an app, where the victim was asked to activate the app and keep it running for a minimum of 30 seconds, most likely to give them enough time to create an account through the referral. The downloaded app did not appear malicious, but it asked users to provide access to sensitive permissions and displayed an excessive number of ads through hard-to-close popups. In other cases, the landing sites also hosted ads from an online advertising network that technology companies marked as suspicious, and which triggered a different redirection chain when clicked.

#### IV.C.2 IP crime

For an IP-infringing business dealing with the marketing of IP-infringing goods, the key to the business model is not only the development of a properly functioning app, but also the physical goods themselves. However, the IP crimes that may arise from the marketing of IP-infringing goods may extend beyond the marketing and sale of IP-infringing goods themselves. As such, it is important to mention the possibility of non-delivery of marketed goods to users. Ultimately, the business model of marketing an IP-infringing product without the capacity to fulfil the delivery, falls under the fraudulent business model (see V). In principle, the two business models can be combined, varying based on the delivery of products or lack thereof. In the same vein, superapps and mini-apps, can be misused by IP criminals to facilitate IP infringement in a similar respect.

<sup>94</sup> Ryan Williams, Red Points (n.d.), [Rogue Websites and cybersquatting](#), accessed on 5 March 2023.

<sup>95</sup> Bill Toulas, Bleeping Computer (2022), [42,000 sites used to trap users in brand impersonation scheme](#), accessed on 6 March 2023.

#### IV.C.2.a Apps marketing IP-infringing goods

Some apps may be created and designed for the specific function of marketing IP-infringing goods. The appeal of IP-infringing physical goods is typically their lower price point. The caveat is usually a higher health and safety risk since IP-infringing goods are not subject to the same product specifications as legitimate goods.

Sellers can post infringing listings through their newsfeeds and receive messages from people in their network if they prefer to remain anonymous. Some of these profiles may promote content with the unauthorised use of trade marks or copyrighted materials<sup>(96)</sup>. No one can look up these messages or listings using search engines because they are not indexed. However, IP criminals have the option of posting publicly, which brings in more hits<sup>(97)</sup>. There have been three major apps in the marketplace that focused on marketing IP-infringing products; one of them was the Vova app.

The Vova app was involved in one of the most relevant cases of apps marketing IP-infringing goods. It was a Hong Kong-based marketplace that no longer exists but was active on a website and on the main official app stores. When searching for a brand name on the website, infringing content was not identifiable, and no IP-infringing goods listings appeared as they were not indexed. However, if the app was downloaded on an Android device, searching for a brand name in the app redirected the customer to numerous listings of IP-infringing goods. The catch

was that when the user clicked on IP-infringing goods listings on the app, a webpage would open in their browser, and with this URL the user could access the listing. The only purpose of the app was therefore to avoid detection. When opened, it resembled any online shopping marketplace, with various categories, currency options, and languages, and a search bar for users to find the products they desired. The banner that opened on the landing page displayed sales offers and the 'bestseller' page, so that users could begin purchasing immediately.

Another of the apps identified was characterised as the 'new Vova' app following the latter's takedown. A marketplace in the form of a website and an app that could be found in the official app stores, providing the same suspected infringing products as the Vova app did. In the app store, the app has a rating of 3.4 out of 5 stars; there are many negative reviews indicating issues such as bad customer service and the inability to return products after purchase. However, the screens within the app store market a different reality to users, promising quality



*What is interesting is that many IP criminals have pushed the IP-infringing goods to apps and away from websites. If you search the website there is nothing illegal. The illegal goods appear only in the app, so the consumer needs to have the app downloaded in the phone to see the illegal products for sale. It is almost as if the criminals know brand protection departments are monitoring the traffic on the website. It is not just in the fashion industry, but consumer health products also.*

IP crime expert

<sup>96</sup> Bill Toulas, Bleeping Computer (2022), [42,000 sites used to trap users in brand impersonation scheme](#), accessed on 6 March 2023.

<sup>97</sup> Ibid.



brands at factory prices. The app assures users of quality items that come at a ‘real bargain’, even more so when using the ‘various coupons’ that the platform offers.

The last app identified is a marketplace that attracts customers with branded products, apparently at very reasonable prices. The marketplace is available in the form of a website and the app is available in the main app stores. It is marketed on social media platforms or through encrypted instant messaging and voice over internet protocol (VoIP) apps. On numerous occasions, the app’s users have complained that they have paid for products that have not arrived (see ‘fraudulent non-delivery’ below and in V.C.3), or they have mentioned poor customer service; some even claim that the logos of the alleged branded products differ greatly from the originals; the brand has consequently been suspected of also marketing IP-infringing goods.

#### IV.C.2.b Production and distribution of IP-infringing physical goods

In the distribution of IP-infringing physical goods, all means of transportation are used. Small parcels, particularly those sent via postal services, account for the majority of seizures, which presents a considerable enforcement difficulty. On the other hand, over half of the global value of counterfeit seizures in 2019 was made up of counterfeits delivered by container ship.

With regard to import and wholesale, illegal business models in the physical goods sector can be found in illegal supply chains that infiltrate legal supply chains, through social media or encrypted instant messaging and voice over internet protocol (VoIP) apps marketing, and e-commerce apps and websites. Global supply chains are currently under a great deal of pressure as IP criminals use these channels to their advantage. Moreover, in recent years, the rise of e-commerce and customers’ reliance on it have provided numerous options for firms to develop their clientele and boost revenues. The same opportunities have also been made available to IP criminals<sup>(98)</sup>.

*International judicial cooperation is, in theory, incredibly powerful, but in practice you need the right people, the right language, a willingness and a high degree of competence. Trying cases between countries that do not have a treaty can be very difficult.*

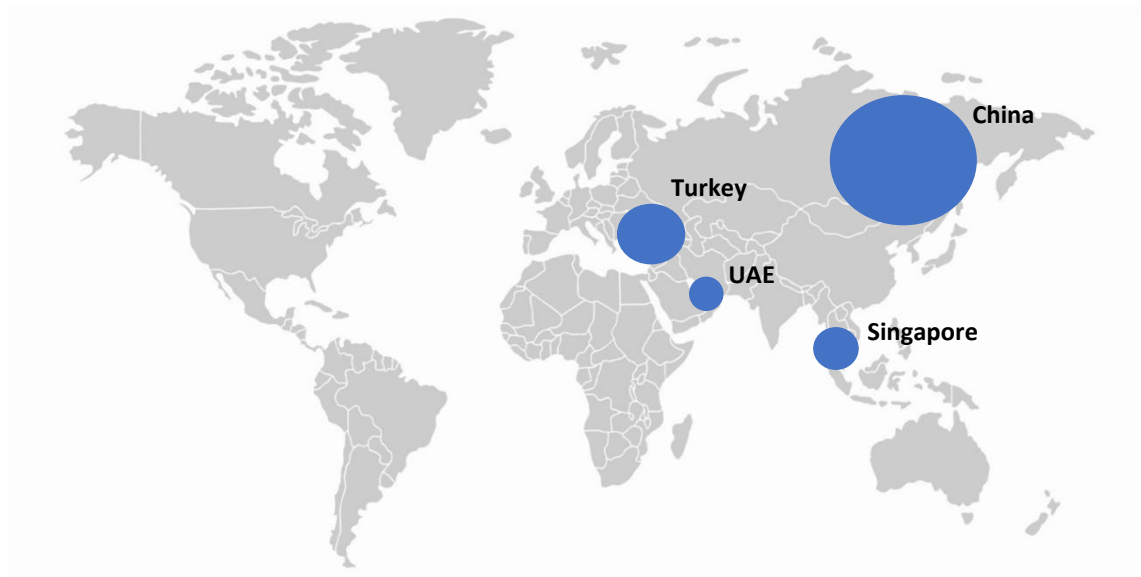
IP crime expert

Although some IP criminals operate their own illegal supply chains, it can be easier to infiltrate legal supply chains, like those that are e-commerce-based and promote direct-user interactions, where IP criminals promote, distribute, or sell their products, which mostly consist of IP-infringing goods.

<sup>98</sup> UKIPO (2022), [Intellectual Property Counter-Infringement Strategy 2022 to 2027](#), accessed on 10 March 2023.

In terms of the production and distribution of goods that infringe IP <sup>(99)</sup>, there are a few countries that have been identified to primarily manufacture these IP-infringing goods. The following graphic is based on an OECD / EUIPO report <sup>(100)</sup>.

### Item 38. Primary provenance for IP-infringing products



Currently, in the new technologically fuelled IP crime ecosystem, the most worrying challenge is that it is more difficult for end users to identify whether they are buying something genuine or IP-infringing.

An example of a case representing a serious risk to safety is the production of trade mark-infringing chainsaws. According to the company in question itself, strict quality and safety standards are among the qualities that define their legitimate products, unlike imitations <sup>(101)</sup>. On their own website, they state that the IP-infringing machines frequently malfunction after only a short period of use, and because spare parts are not readily available, they cannot be fixed. Moreover, they refer to safety-critical components that may be broken or not present at all in these IP-infringing products, giving the example of

*the hand guard for the automatic chain brake - the most important safety device on a chain saw – which was found to be broken when one counterfeit saw was unpacked.*

<sup>99</sup> A joint study by the EUIPO and OECD on '[The Global Trade in Fakes](#)', revealed that, in 2019, global trade in counterfeits amounted to EUR 412 billion in 2019, corresponding to up to 2.5% of world trade. Specifically, EUR 119 billion worth of counterfeit goods were imported to the EU, representing up to 5.8% of total imports from outside the EU.

<sup>100</sup> OECD / EUIPO (2023), '[Risks of Illicit Trade in Counterfeits to Small and Medium-Sized Firms](#)'.

<sup>101</sup> STIHL (n.d.), [STIHL warns about imitation](#), accessed on 27 July 2023.

#### IV.C.2.c Superapps and mini-apps

A new trend in the last two decades has been the development of superapps and mini-apps. While superapps are apps that encompass a number of functionalities, as displayed in the Item below, mini-apps are related but independently developed apps that facilitate the integration of other services. Both have been identified for potential misuse in the marketing and sale of IP-infringing goods.

The relation between the two apps is close-knit: superapps serve as hosts for mini-apps and are available on several operating systems. Mini-apps require superapps to run and can run in different operating systems (OS), as long as the superapp is developed to run on that OS<sup>(102)</sup>. A mini-app can be accessed directly via the superapp and allows users to access additional functionalities that may not be available in the general functionalities of the superapp. However, for a mini-app to be offered, the owner of the superapp must authorise its publication on their platform<sup>(103)</sup>. Given the interconnected nature of superapps and mini-apps it is evident that they are more popular within one region. In Europe, users are more accustomed to various apps with varying functionalities, available for download from select sources (see III.B for app gateways).

*The closed environment in super apps is expected to make it more difficult to detect infringements. Counterfeiting and other trade mark infringement are common occurrences in these types of apps, a problem exacerbated by the apps' privacy settings. Sellers are also able to hide their identities and locations, selling only to people with whom they have established a direct connection.*

IP crime expert

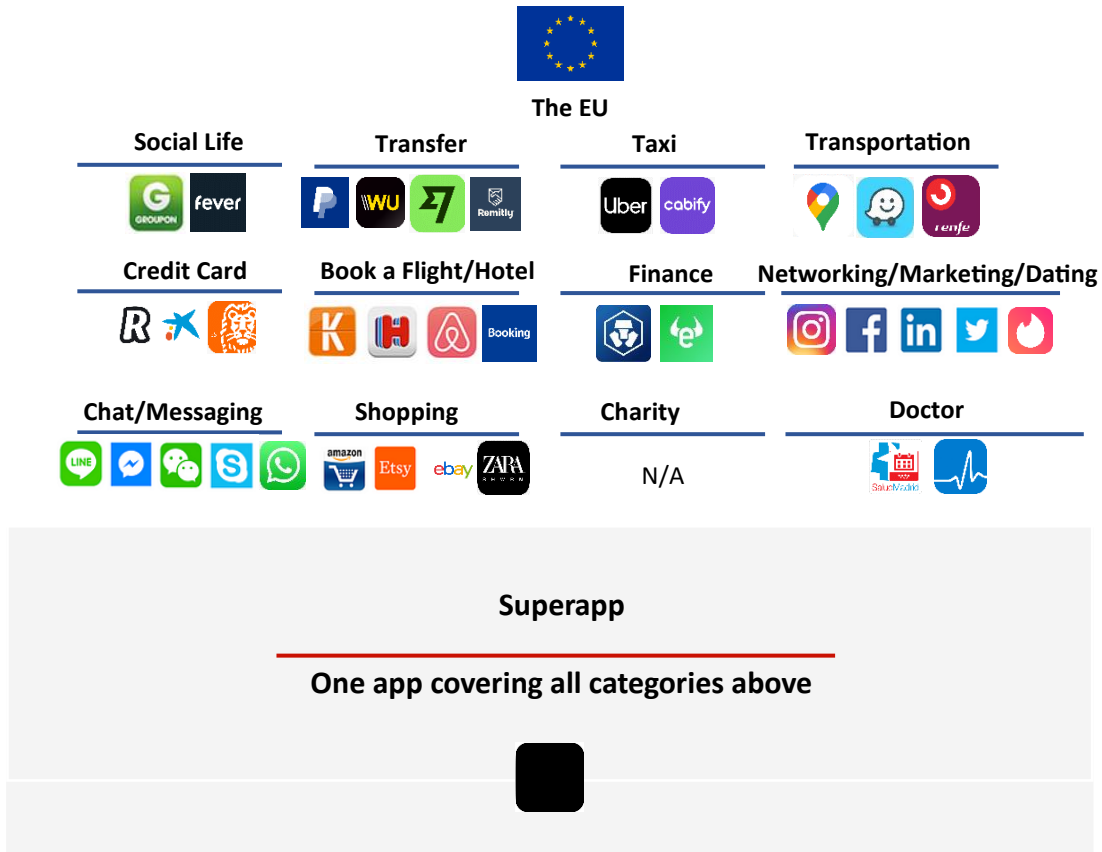
---

<sup>102</sup> Steiner, Thomas (2021), '[What are mini apps: Building blocks and compatibility](#)' accessed on 18 March, 2024.

<sup>103</sup> Arambule, Wina (2022), '[Difference between Super Apps, Mini Apps and Mini Programs](#)', accessed on 18 March, 2024.

The following graphic is built on UX Collective (104).

Item 39. Different apps with varying functions v  
one superapp covering all listed functions



By comparing superapps and the individual-function apps that are more popular in Europe, it is evident that Europe has a vast number of apps that cater to different categories of needs, such as social life, social media, dating, credit cards, travel bookings, transportation, finance, shopping, and health, as well as the various instant messaging platforms. The categories are numerous, with multiple players within each giving users a wide array of apps to choose from.

<sup>104</sup> This graphic was adapted from Jessie Chen, UX Collective (2016), '[Everything you ever wanted to know about WeChat](#)' to depict the EU instead of the US.

Since all these functionalities are subsumed into one app, in other regions, these superapps become a ‘one-stop shop’ for all a user’s needs and ultimately remove the need for options. While the convenience may be significant, it also entails a series of challenges for internet users and IP owners. For some brands, a superapp’s closed environment and system pose a risk and make it difficult to detect IP infringements. The privacy settings in these apps may facilitate trade mark infringement through fraud and the marketing of IP-infringing products. By marketing to people with a direct connection to the app, sellers can conceal their identities and locations, unlike public-facing websites that facilitate transactions among strangers and display instances of trade mark infringement and public use<sup>(105)</sup>.

#### Item 40. Important emerging trend – superapps

##### Important emerging trend: superapps



Superapps are ‘all-in-one’ apps that combine multiple app functionalities and bring them into one platform, eliminating the need to download numerous programs to carry out different tasks. They provide multiple services like social messaging, e-commerce and payment, and financial transactions in one place<sup>(106)</sup>.

The term ‘superapp’ was first introduced to refer to a Chinese communication app that launched more than 10 years ago as a messaging app and has now grown into a superapp with 1 billion users, mainly in China. These superapps are still primarily popular in Asia and Africa<sup>(107)</sup>. The concept of mini-apps was conceived in the same place, in connection to superapps, and only function within the superapps. Mini-apps ultimately provide additional functionalities to users that may not be included within the superapp itself.

#### IV.C.2.d Fraudulent non-delivery of physical goods

The marketing of IP-infringing physical goods can sometimes be part of the IP criminal’s scheme of fraudulent non-delivery of these goods. In these cases, the internet user purchases physical goods in an app, whether an IP-infringing app or legitimate app, the IP criminal advertising the product has no intention or means of delivering the goods to the users. Ultimately resulting in fraud, as such this practice overlaps with fraudulent business model (see V).

<sup>105</sup> Corsearch (2020), [4 Things IP Professionals Need to Know About WeChat](#), accessed on 14 March 2023.

<sup>106</sup> Lori Perri, Gartner (2022), [What is a Super App?](#), accessed on 9 February 2023.

<sup>107</sup> Deloitte in The Wall Street Journal (2022), [Forecasting the Future of Super-Apps](#), accessed on 14 March 2023.

Item 41. **Law enforcement investigative strategies relevant to  
marketing of IP-infringing goods**

**Law enforcement investigative strategies relevant to  
infringing business model 2**

When law enforcement authorities are investigating an app that is suspected of marketing IP-infringing goods, there are at least four strategies that may be implemented as part of the investigation.



The **follow the goods** strategy will aid in extending the investigation beyond the mere prevention or disruption of the marketing and sale of IP-infringing goods. Rather, the focus is on investigating the supply chain to identify the IP criminals, link offline and online marketing to physical storage and distribution, and correlate different means of online and offline marketing. The aim is to ultimately dismantle the whole supply chain, or at least significant parts of it.

The **follow the pattern** strategy may connect individual occurrences of the marketing of IP-infringing goods facilitated by apps to larger IP crime operations. In this strategy, clusters of IP crime can help to uncover the full scope of the operation. In some cases, an infringing app operation may seem isolated from other operations, but investigating the infrastructure, ownership and money flow of the operation may lead to connections between several apps. Some investigative techniques involved in 'follow the pattern' include, but are not limited to, the use of internet investigations (e.g., open-source intelligence (OSINT), and obtaining data from internet intermediaries).



The **follow the money** strategy involves identifying the infrastructure related to money inflow, identifying the persons involved, and disrupting the money flow. Doing so will also require understanding the tools used to obtain money, whether through electronic, cryptocurrency or traditional bank mechanisms. Following the money may also entail retrieving evidence related to payments and supporting future money laundering charges.

The **follow the person** strategy focuses on identifying the various IP criminals and their affiliations and identifying how they cooperate and collaborate as an organised crime group. Beyond individuals, this strategy also identifies limited-liability companies, foundations or associations used by IP criminals to facilitate their operation and observes the movement of targeted persons to uncover the locations in the supply chain.



Read more about business models related to marketing of IP-infringing physical goods in other reports in the infringing business model series <sup>(108)</sup>.

### IV.C.3 Criminal gain

Although advertising and fraud revenue may be used to generate criminal gain from IP-infringing apps that involve physical goods, the most common source of revenue in these cases is sales revenue. Sales revenue may be generated through the unauthorised sale or distribution of IP-protected materials, as well as in cases where the goods or services

<sup>108</sup> In the [IBM phase 5](#) report chapter 5, there is a description and analyses of production and dissemination of IP-infringing goods. The [IBM phase 4](#) report specifically analysed vendors of IP-infringing goods on e-commerce platforms.



promised are not delivered (in such cases, there are evident overlaps with business model 3 on IP infringement for malicious and fraudulent purposes see V).

#### Item 42. Enforcement and investigative measure – financial investigation

### Enforcement and investigative measure: financial investigation



A financial investigation is a combination of usually quite common and basic investigative techniques, methods, and tools (including cryptocurrency investigation) aiming at disclosing account information, payments, and any related data, information, intelligence, and evidence. Financial investigation into an IP crime will be relevant in almost any case. The ‘follow the money’ investigative strategy is therefore applicable in practically all IP crime cases.

Financial investigations can assist in:

- determining the extent of the crime, including historic illegal activities;
- gathering evidence in operations related to fraudulent use of advertising (see III.C.3.a) as well as cryptocurrencies (see V.C.3);
- identifying physical and legal persons as well as OCGs involved in the crime;
- disclosing infrastructure and intermediaries misused by the IP criminals;
- uncovering the supply chain of physical goods and the delivery of digital streams.

One of the main drivers for IP criminals is the generation of revenue. Consequently, it is imperative to seize the assets of IP criminals and endeavour to forfeit these proceeds of crime. The confiscation of an IP criminal’s assets can potentially be a greater punishment than a custodial sentence. However, even in IP crimes that did not generate a direct revenue, a financial investigation into the infrastructure used will often be eventually very valuable. An important part of financial investigations is therefore the freezing of ongoing payments or deposits in accounts.

Furthermore, the identification of these assets and their source can lead to alternative offences including money laundering. Both physical and electronic evidence (see more about electronic evidence in VI.A.1) can assist in identifying assets and their sources.

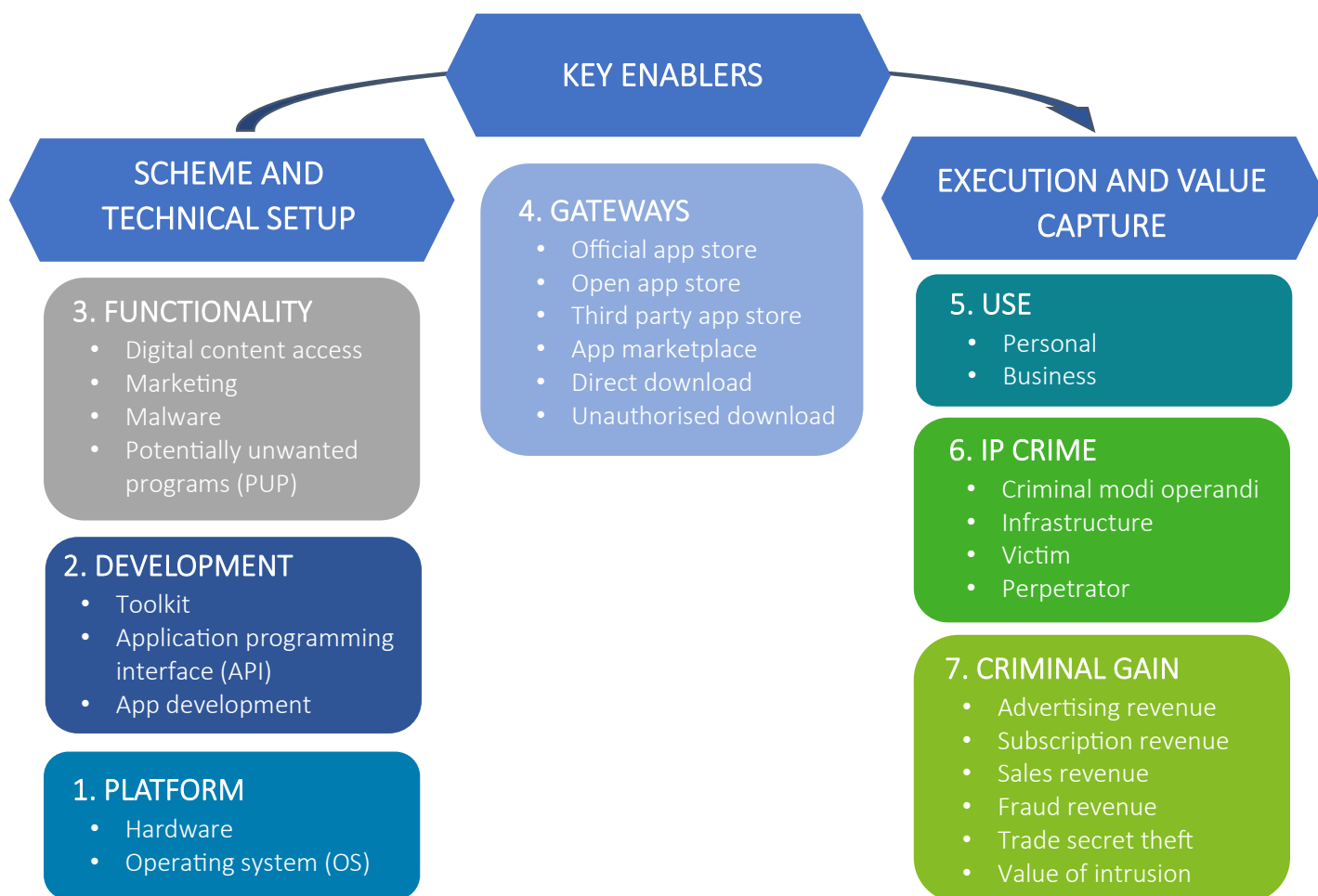
## V Infringing business model 3: IP infringement for malicious and fraudulent purposes



The business models applied by IP criminals and other cybercriminals, including developers consciously developing malicious and fraudulent apps, to obtain money or other gain by way of deceiving app users, accessing their personal data or compromising their devices, will usually entails the unauthorised use of various IP, including the trade marks of others.

The description of the business models follows the content of the arc of IP crime related to apps. The business models described in relation to IP infringement for malicious and fraudulent purposes has a number of overlaps with business model 1 related to infringement of copyright-protected digital content (see III), business model 2 related to marketing of IP-infringing physical goods (see IV), and business model 4 related to trade secret theft (see VI).

#### Item 43. The arc of IP crime related to apps



#### V.A Scheme and technical setup



Malicious and fraudulent IP-infringing apps that exploit technical vulnerabilities and apply social engineering techniques for direct or indirect financial gain have various means of development and dissemination, and widely varying functionalities.

## V.A.1 Platform

The scheme and technical setup of these IP crimes refers to the methods and instruments used by IP criminals to infringe IP – in this business model – in a way that is malicious, fraudulent, or both. The methods, content sources, and setup that IP criminals use are all part of the scheme.

The technical setup is similar to that used in the digital content business model (see III.A.1). It involves various actions, such as choosing the platform used to perpetrate the crime, developing the fraudulent app and its functionality.

Within the setup, an IP criminal may attempt to take advantage of the hardware developer by exploiting flaws or vulnerabilities in the hardware or software. As part of this exploitation, the following may be used.

- Hardware trojan: a case where any hardware (integrated circuit) is modified with malicious intent during a production stage, regardless of how harmless the modification seems. Manufacturers who outsource any of their components to an outside factory have been concerned by this problem.
- Reverse engineering: the process of learning about system behaviour and hidden internal functionality by methodically analysing each component (e.g. parameter analysis, output analysis, and input-output relationship). This tactic is used in both hardware and software IP attacks (see III.A.2.c).
- Unauthorised production: a result of outsourcing, or cloning, hardware (mainly integrated circuits or ICs) and not monitoring a remote foundry. Unauthorised productions enable intruders to examine ICs and reverse engineer them, or even embed the attacker into the hardware.

Hardware metering or IC metering, hardware obfuscation, split manufacturing, IC camouflaging, logic locking, fingerprinting, and watermarking are some of the main generic hardware-oriented defences against hardware-IP attacks. Additionally, hardware-IP security research has recently seen an increase in the use of machine-learning models to detect anomalies in hardware IP and devise methods to secure it (<sup>109</sup>).

---

<sup>109</sup> Ashraful Tauhid, Lei Xu, Mostafizur Rahman, and Emmett Tomai, '[A survey on security analysis of machine learning-oriented hardware and software intellectual property \[Issue 3, Volume 1\]](#)', accessed on 14 April 2023.

## V.A.2 *Development*

The development of IP-infringing apps related to IP infringements for fraudulent and malicious purposes is to some extent done in the same way as described in the chapter on infringement of copyright protection digital content (see III.A.2).

*One of the biggest threats posed is IP-infringing apps that look like legitimate apps. Many internet users will search for an app in their app store and can inadvertently download something believing it is legitimate and unarmful, when it is in fact not.*

IP crime expert

However, it can also be noted that the strategies employed by IP criminals in the world of cybercrime are constantly evolving, the *modi operandi* usually involve replicating the functionalities of legitimate apps from traditional providers. Ultimately, this is done to deceive unsuspecting internet users into downloading and installing unsafe and malicious IP-infringing apps (<sup>110</sup>). It is critical for internet connected smartphone users to be aware of these hazards, as IP criminals are becoming more inventive and sophisticated in their strategies, which combine social engineering with technical exploitation. In addition, it is imperative to safeguard devices from these threat actors who are always looking for new ways to target their victims and steal crucial data for their own malicious purposes (<sup>111</sup>).

## V.A.3 *Functionality*

Apps can contain malware, or malicious software, which can be used to steal user data, disseminate spam or phishing emails, or cause other harm to users. The desire to access infringing content is used as a trigger or incitement to download and install software, plug-ins and extensions that can be malicious (<sup>112</sup>). By downloading these tools, users expose their personal information and put themselves at risk of having their data stolen and used for other purposes without their knowledge, which could lead to an overload of unsolicited advertisements, and other illicit activities.

---

<sup>110</sup> Akshay Singla (2023), '[Beware: Fake Applications are Disguised as Legitimate Ones](#)', accessed on 9 June 2023.

<sup>111</sup> Hack Control (2023), '[Mobile App Fraud](#)', accessed on 25 March 2023.

<sup>112</sup> [Shampoo malware](#), accessed on 12 September 2023.

### V.A.3.a Fraudulent functionalities

As IP-infringing fraudulent apps are becoming common and are making their way into official app stores, functionality can vary depending on the app; several business models for fraudulent apps have developed over time, including the following<sup>(113)</sup>.

- The placebo app: this type of app has no functional effect and is just a façade – when the user pays for the intended product or service, the application provides no product. The IP criminal simply keeps the money when users pay for the download.

As early as 2008, an app was released on a major official smartphone app store priced at USD 999.99; the description read 'I Am Rich, I Deserve It, I Am Good, Healthy & Successful'. In the app store, the app was displayed with its icon, which was a red ruby, below which was the app's name and the category 'Lifestyle'.

The app's functionality was exceedingly basic, with no practical use. Customers who bought the app and opened it were met with a message and the image of a red jewel. The app did nothing more than display the image and text; there were no extra features or functions. It was intended to be a status symbol for wealthy people who wished to flaunt their wealth, according to the developer. Many, however, believed the program to be an attempt to profit from unaware users' curiosity or lack of awareness because of its high cost and lack of actual benefit<sup>(114)</sup>. Within 24 hours of its debut, Apple deleted the app from the app store, although within that brief window, a few users apparently bought it before it was removed. Later, the developer produced an almost identical but less expensive version of the app that cost USD 599.99, which again had no function.

- Apps packed with adware: this type of IP-infringing app contains adware, which automatically bombards the unsuspecting user with a multitude of pop-up advertisements in order to generate advertising revenue. Oftentimes, these ads are from malicious operators and can expose the users to more risk. The ads are not typically ordinary ads rather more malvertising to promote more malware installation or attack. Moreover, these apps may have a cloaking feature built into their code which prevents the creation of a shortcut icon on the home screen, making it very challenging to locate and remove the ads. For an example see, IV.C.2, the case of the malicious for-profit group that promoted adware apps, among other things.

*Generally, most IP criminals want to move from web to apps because it costs less and is more difficult to investigate. Criminals also move to apps because they can lure in more customers, with more control and stronger targeting techniques. Malicious apps also ask for permissions, so after luring in the customers, they can gradually ask for more permissions and gain access to more and more sensitive information.*

IP crime expert

<sup>113</sup> Fraud Watch (2023), [The Rise of the Fraudulent Mobile App](#), accessed on 25 March 2023.

<sup>114</sup> Antoni Żółciak (2017), [I Am Rich: The Story Of The World's Strangest Mobile App](#), accessed on 10 June 2023.

### V.A.3.b Malware and potentially unwanted programs (PUPs)

Apps can contain malware, or malicious software, which can be used to steal user data, disseminate spam or phishing emails, or cause other harm to users. This behaviour can affect both legitimate and IP infringing apps alike. However, IP criminals may use apps that disseminate illegal content to distribute malware to internet users which is not only unlawful but also detrimental to these users and a violation of app store standards.

- **Stealth malware:** this type of app is particularly harmful, as it infects the IT system with malware intended to steal confidential, financial, and personal information. Many pieces of malware can identify the make, model, unique ID, and precise location of the compromised device on which they are installed.

As an example of a stealth malware app, a gaming studio that owns several apps that have been available for years on the Google Play Store was discovered to have been infecting numerous devices in 2017. The interface of the apps containing malware resembled a cute, anime-style cartoon girl with pink hair holding a box of sushi – seemingly unthreatening. The Android symbol was also prominent on the app’s interface to indicate to users that it was intended for Android devices.

*There is a ‘multiheaded snake phenomenon’, whereby a developer uploads hundreds of apps with the same malicious functionality.*

IP crime expert

The apps were camouflaged as innocent and trustworthy programs, such as cooking and fashion games that generated plenty of downloads<sup>(115)</sup>. Once downloaded and activated, the malicious apps operated covertly, by clicking on the advertisements displayed on infected devices without the user’s knowledge. The developers received fraudulent income as a result of this advertisement-clicking activity.

In addition to the IP infringement, the capability of this IP-infringing app to steal private data from infected devices was very concerning. The malware was created to establish a connection with a remote server, enabling it to download and run more malicious programs. The app was able to access sensitive user data, including login information, financial information, and personal information, thanks to this secondary code.

Apps can also provide potentially unwanted programs or content, for example software that provides advertisements. This software is not always characterised with containing malware programs and may just be a nuisance or used to generate fraudulent ad-revenue (see V.C.3)<sup>(116)</sup>.

<sup>115</sup> Christine Smith, TunesGo (2021), [Judy Malware: List of Infected Android Apps](#), accessed on 10 June 2023.

<sup>116</sup> EUIPO (2018), [‘Identification and Analysis of Malware on Selected Suspected Copyright-Infringing Websites’](#).

### V.A.3.c Other functionalities

Other functionality challenges that law enforcement may face are the following.

- Geo-blocking techniques: Infringing developers can apply geo-blocking techniques, where infringing content is only shown in target countries. An example would be the case of a provider in China that ensures the app is not available in China, but only where the target audience is located (see V.A.3.c). There can be additional blocking techniques, depending on the specific device hardware, version of the operating system, other installed apps, and existence of alternative accounts on the device.
- Apps blocking the screenshot functionality: the technique to restrict users from taking screenshots while using the app may be a feature of some infringing apps. By preventing users from screenshotting IP-infringing content, they hope to make it more difficult for copyright owners to detect and report infringement.
- Apps that hide the identity of the IP criminal: IP criminals operating apps may hide their identity under several layers of obfuscation techniques. This strategy makes it difficult for IP owners and law enforcement to identify and investigate the IP criminals.

*Criminals need to hide their identity. It's the most important part of a criminal plan. Likewise, disclosing identities is the most important job for an internet investigator. The good thing is that the criminal shall only make one mistake to get caught. That is the great opportunity to cyber-investigations.*

IP crime expert
- Illicitly putting different entities in their terms and conditions (T&C): by adding erroneous information or different businesses in their T&Cs, infringers engage in misleading activities to deceive users and authorities about the real controller of the app, making it more difficult to enforce IP.
- Fraudulent non-delivery and fraudulent advertising: some IP criminals may use apps to falsely promote goods or services to consumers with no intention of delivering the product. The advertised product can either relate to services or IP-infringing physical goods, in which the latter may be more common since users will only detect the fraud at a later stage, ultimately demonstrating how this practice may overlap with business model 2 on marketing of IP-infringing goods (see IV.C.2).
- Misuse of permissions: an attack vector that may be used by third party applications is the misuse of permissions given by the operating system (OS) on the device. When an app is being installed, on a smartphone for example, it can request a certain set of granular permissions to access internal hardware or software. An app that shows location on the map will most likely ask for the GPS coordinate and access to the Internet to update the map. However, adversarial actors tend to put up tens of

unrelated permissions like sending or receiving calls, reading SMSs or making paid phone calls.

Moreover, IP criminals occasionally operate in jurisdictions with limited enforcement of IP laws, or other relevant laws, or little participation in international enforcement initiatives. They might exploit this to establish fictitious businesses, entities with no assets or shell companies, or have no physical presence. This makes it challenging to file lawsuits and seek compensation from infringing activities, and unlikely that criminal enforcement measures or investigations will be initiated.

#### Item 44. Important emerging trend – geo-blocking

### Important emerging trend: geo-blocking



Apps differ from websites in the new geo-blocking techniques applied by IP-infringing developers to block content based on geographical location. More specifically, geo-blocking entails preventing access to a resource that is accessible across a network based on the alleged location of the system or user attempting to access it. Blocking refers to system-level blocking, such as allowing the app to reject or ignore the access attempt, or network-level blocking, such as deleting IP packets<sup>(17)</sup>.

Criminals may use geo-blocking techniques to facilitate IP infringement on an app. Those wishing to participate in unlawful actions associated with IP infringement may manipulate geo-blocking, which aims to restrict unauthorised access to copyrighted content. Criminals might permit access to infringing content based on location or use geo-blocking as an obfuscation technique to avoid law enforcement detection. Additional blocking techniques may also be applicable depending on the hardware of the specific device, version of the operating system, other installed apps or the existence of alternative accounts on the device. Geo-blocking can be used by criminals in the following ways.

- Infringement of copyright-protected digital content: When IP criminals produce or acquire copyright infringing copies of content, geo-blocking can be used to limit distribution to regions where copyright laws may be more lenient.
- Setting up servers in permissive jurisdictions: to host apps or content that infringe IP, criminals may set up servers in nations with lax IP enforcement and then use geo-blocking technologies to prevent access to regions with more stringent IP laws.
- Selling unauthorised copies: criminals might exploit geo-blocking to disseminate illegal copies of widely used apps or copyrighted content to specific markets. These illegal products may only be available to users in areas where official equivalents are difficult to find or inaccessible.
- Avoiding legal action: IP criminals try to avoid being discovered and facing legal repercussions for their IP-infringing actions. They believe restricting access based on location will make it harder for IP owners to take legal action.
- Traffic monetisation in permitted areas: IP criminals may reroute users to earn money through advertising clicks, affiliate marketing, or other monetisation strategies with a lower risk of legal repercussions.
- Limited-liability exploitation: by employing geo-blocking to concentrate their operations within particular jurisdictions, criminals can establish businesses in areas where legal liability for IP infringement is minimal or non-existent.

<sup>17</sup> John Burke (2023), [Geo-blocking](#), accessed on 26 July 2023.



## V.B Key enablers: gateways



The key enabling gateways providing access to download an app related to IP infringements for fraudulent and malicious purposes are the same as described in the chapter on infringement of copyright protection digital content (see III.A.2).

From an enforcement and investigative perspective, the gateway will usually be of unique importance. App stores and app marketplaces might have in place precautionary, preventive, and proactive measures to avoid apps enabling IP crime, and there will often be different types of evidence available from the gateway, including basic subscriber information, transactional data, involved IP addresses, correspondence, and payment information. Read more about internet investigation in V.C.2.b, and digital evidence in VI.A.1.

There are several precautionary measures that are implemented within each gateway to prevent IP criminals enabling IP-infringement through apps (see III.B.1).

## V.C Execution and value capture



IP criminals are always discovering new ways to defraud internet users by techniques and social engineering enabled by infringing IP, mainly trade marks.

By deciding how the app can be used and the most ‘profitable’ type of infringement, infringing apps can generate profit in a variety of ways.

### V.C.1 Use

In the case of fraudulent apps, IP criminals usually target individual users, or groups of individual users, that download apps for personal use. Ultimately, the consumer is expecting one kind of app, but receives another app entirely; or in some cases, the user receives nothing at all. The ultimate goal of these IP-infringing apps is to make the consumer download and use the app with one set of expectations. The fraud element becomes relevant when the user’s expectations are not fulfilled. The IP criminals can thereby receive illicit payments, gain access to personal data, or obtain another economically valuable advantage.

*Law enforcement authorities are usually ‘victim-focused’. Therefore, IP crimes should demonstrate the economic damage inflicted the victim in order for law enforcement to get more involved. The financial gain obtained by serious and organised criminals are good hooks for law enforcement.*

IP crime expert

Item 45. **Enforcement and investigative measure – raising awareness**

**Enforcement and investigative measure: raising public awareness**



**Public awareness activities** are essential to decrease the demand of IP-infringing products from the side of the user. Promoting a better knowledge of IP and their implications within the app ecosystem can be facilitated through public awareness campaigns, educational and training initiatives.

European institutions get involved in these activities by funding relevant initiatives and working with the Member States to raise citizens' awareness of the importance of IP, the need to respect it, and the potential damages and risks these infringing products can have on society (<sup>118</sup>).

Public awareness campaigns can also be an efficient method for disseminating information about the risks associated with using infringing apps, differing depending on the target audience. For younger audiences (Gen Z and Millennials), influencers and social media platforms such as TikTok, Snapchat, Discord, and Instagram are crucial, with visual content demonstrating the dangers of these apps being particularly effective. Traditional media like online newspapers are more suitable for reaching a mature audience (Gen X and Boomers), along with radio due to its low dissemination costs and broad reach. To reach the general public, short, animated videos with subtitles conveying the risks of using infringing apps, along with infographics, can be effective, with emphasis on utilising platforms like YouTube for maximum exposure. Additionally, consumer and youth associations, as well as law enforcement agencies, can play a significant role in raising awareness and disseminating information about the dangers of infringing apps.

Education and training programs exist for IP enforcers and as part of IP educational programs for young at secondary and tertiary education centres can also include references to apps, since currently it is not a typical product that is generally associated with IP protection.

*Public awareness is of utmost importance. Companies that focus on enforcement should also focus on campaigns and educational material to spread public awareness. Not only is it important to spread public awareness among internet users – children as well as adults – but also teachers, academics, law enforcement authorities and policymakers.*

IP crime expert

### V.C.2 IP crime

The crime within this business model focuses on the act of using someone else's IP to deceive or defraud others for financial gain. Just like the crimes described previously, this model also causes damage to the reputation of the company or brand affected and can result in considerable financial losses for the IP owners.

To combat the abovementioned crimes, various measures need to be in place. Moreover, it is of the utmost importance to raise awareness among users about the dangers of being misled by apps into accessing fraudulent online services and schemes.

<sup>118</sup> EUIPO (2020), [Status Report on IPR Infringement, June 2020](#).

### V.C.2.a Threats of IP-infringing fraudulent apps

As fraudulent apps grow more prevalent, they present serious challenges for both individuals and corporations. Falsifying personal information, assuming false identities, or lying about one's background are a few examples of the many ways that fraudulent apps can be created and disseminated. Although individuals are the primary target for such IP crime, IP-infringing fraudulent apps may also target the activities of corporations. In either case, the surge of fraudulent apps highlights the necessity of thorough identity verification procedures and heightened attention. If not done correctly, two of the most pressing challenges posed by these apps are fraud and cyberattacks, which can occur in many forms; some examples are given below.

### V.C.2.b Domain Name System (DNS) abuse

Any behaviour that takes advantage of vulnerabilities or abuses the DNS to further harmful objectives is referred to as DNS abuse. Domain name servers are a crucial part of the internet, facilitating the conversion of human-readable domain names into IP addresses that computers can comprehend<sup>(119)</sup>. This type of abuse is not limited to traditional internet use cases: it is also a growing concern for apps. According to the EU study on DNS abuse<sup>(120)</sup>, it is a rising issue for companies, governments, and individuals alike; to counteract it, cooperation is needed between internet service providers, domain registrars, law enforcement organisations, and cybersecurity professionals.

The architecture of DNS abuse can involve botnets and command and control servers (C&C servers), which are used to control communications between attackers and the botnet intended to attack a target by disrupting the DNS. At this point, the botnet can perform any command that the IP criminal requests, which usually means redirecting the user to malware-distributing websites or distributing the malware itself. Usually, an IP criminal will exploit DNS to hide the location of C&C servers and bypass measures used to detect them. In these cases, the IP criminal could conceal all C&C information by using seemingly innocent DNS records<sup>(121)</sup>. However, a relatively new standard, known as the Domain Name Systems Security Extensions (DNSSEC), is aimed at strengthening DNS security and is being implemented by many cloud providers to avoid posing or manipulation of DNS requests.

Depleting the targeted system resource, corrupting data, stopping the DNS system from functioning, or abusing the system to carry out the ultimate attack are some of the objectives of a DNS attack. Four types of DNS attacks can be distinguished: DNS data tampering, DNS data flooding, abuse of DNS, and DNS server structure. The following graphic is an elaboration of work published on Research Gate<sup>(122)</sup>.

---

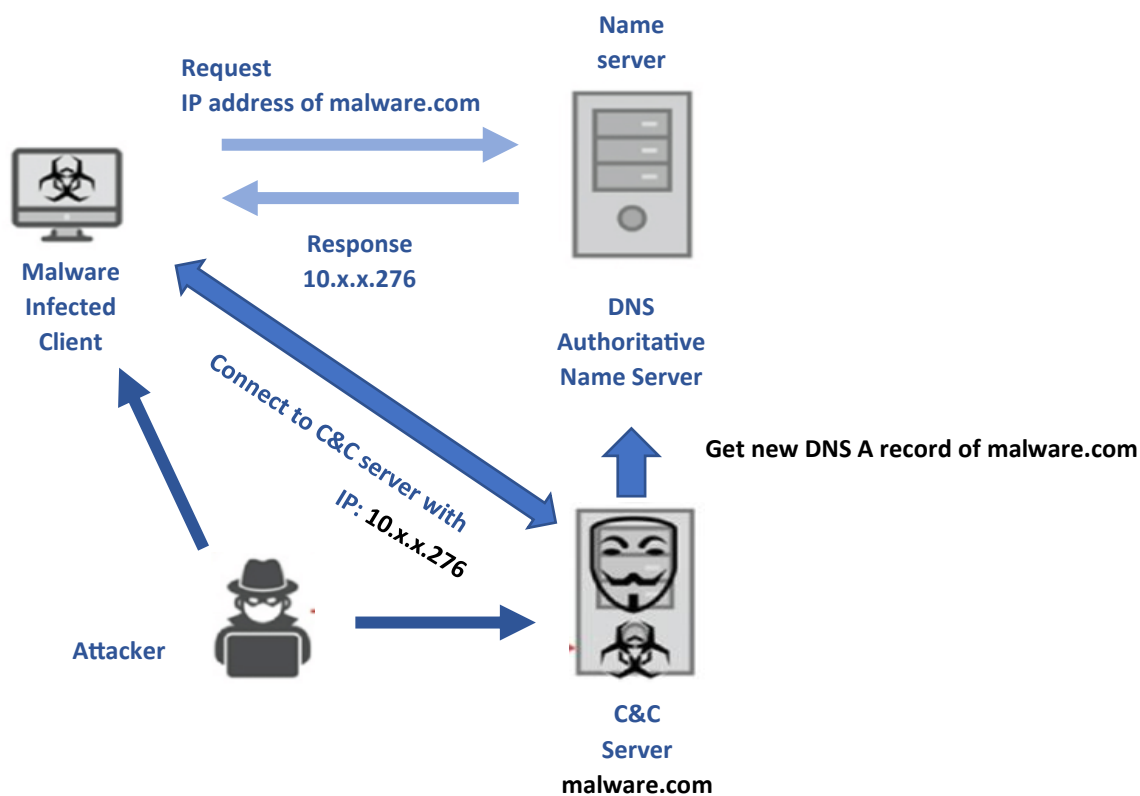
<sup>119</sup> Ahona Rudra (2023), [What is a DNS server?](#), accessed on 25 March 2023.

<sup>120</sup> European Commission, Directorate-General for Communications Networks, Content and Technology, [Study on Domain Name System \(DNS\) abuse, Publications Office of the European Union, 2022](#), accessed on 25 March 2023.

<sup>121</sup> Research Gate (2020), [Demonstrating the DNS attack using abuse of DNS. DNS: Domain Name System](#), accessed on 7 June 2023.

<sup>122</sup> Ibid.

Item 46. **DNS abuse**



As apps can gather private user information, DNS abusers are drawn to them, which might result in data breaches, financial loss, and reputational damage. Whether on websites or apps, DNS abuse can take many forms, such as cybersquatting, typosquatting, phishing, malware distribution, advertising fraud, and malicious code injection.

Item 47. **Enforcement and investigative measure – internet investigation**

## Enforcement and investigative measure: internet investigation

An internet investigation focuses on identifying information, intelligence, data and/or evidence from open internet sources that is actionable, can be used as intelligence or as evidence in a court of law. Some important information to be aware of is:



- Information is volatile so detailed documentation is important.
- The true relevance of information is rarely obvious upon first glance so documenting more than what seems immediately relevant is usually a good idea.
- Corroborate information as much as possible as the internet contains large amounts of false or inaccurate information.
- Sometimes the investigation benefits from pure luck, and such luck can be utilised to detect criminals that can be identified by a single mistake.
- Leverage investigative communities and networks to keep skills up to date and network with colleagues from other countries, which is crucial.
- Be creative and combine techniques and tools to link information, including reverse engineering (see III.A.2.c).

Open-source intelligence (OSINT) is an important part of most internet investigations. The term refers to the collection, analysis, and dissemination of intelligence gathered from publicly available sources. This can encompass sources such as news articles, social media posts, government reports, and online forums. Unlike traditional intelligence-gathering methods, which often rely on classified sources, OSINT focuses on procuring information from sources accessible to the general public. A special area of OSINT is social media intelligence (SOCMINT), which encompasses techniques and tools to extract intelligence from social media platforms.

Internet investigations will normally fall into six phases.

- Phase 1: Defining the objective. In this phase, expectations are clarified, and an investigation plan is developed.
- Phase 2: Preparation. In this phase, a security and privacy hardened workstation is made and audited, and the relevant tools for the investigation are installed and tested.
- Phase 3: Identifying the sources of data. In this phase, the sources that can be investigated are identified.
- Phase 4: Capture. In this phase, intelligence is collected, and all steps are carefully recorded and captured for future reference and documentation purposes.
- Phase 5: Analyses. In this phase, the findings of the investigation are analysed in light of the objective of the investigation. Additionally, the relevant findings are visualised in an easily understandable way.
- Phase 6: Reporting. In this phase, all the previous steps are described, and the intelligence's relation to the crime being investigated is highlighted.

### V.C.2.c Cybersquatting and typosquatting methods used in apps

Cybersquatting is a term usually used to describe the unauthorised registration and use of a domain name that is identical to another's trade mark (see also typosquatting). Typosquatting is usually used to describe the unauthorised registration and use of a domain name that is similar to another's trade mark (see also cybersquatting). Cybersquatted or typosquatted domain names can be used to generate various illicit income.

Methods similar to cybersquatting and typosquatting can also be applied in relation to other types of digital identifiers (e.g., social media profile names and handles, and titles of apps sometimes called app squatting).

In the case of apps, cybersquatting and typosquatting or similar methods can occur in two ways: firstly, when someone registers a domain name that is similar to the name of a popular app with the intention of misleading users and diverting the traffic to their own website or app; and secondly, where the IP criminal creates an app with a similar name, logo or design to that of a popular app with the intention of confusing users and free-riding on the real brands' popularity. In both cases, the app may contain malware, adware, or spyware, harming the users' devices or stealing sensitive information.

*If we look at emerging IP crime and apps, the market is very fragmented. There is consolidation at the top but a lot of fragmentation at the bottom, with a lot of layers of front-end criminals. This makes enforcement much more complicated, challenging, and costly.*

IP crime expert

The fact that IP criminals can create infringing apps imitating a real app is a serious threat to internet users (e.g., where health information and other sensitive data is collected). An example of suspected IP criminals cybersquatting health apps might be when they impersonate legitimate health apps, leading to potential processing of sensitive health data from users who thought the app was legitimate.

A recent case concerning the use of cybersquatting methods concerned a fake version of Signal, a private messaging app, which was disseminated through traditional app gateways. This app appeared to be linked to a government-led spy operation. The IP criminals did not stop at uploading their version on one app store but disseminated the app through many gateways. The functionality of the fake app was the same as the legitimate version, but its hidden aim was to spy on the communications of the real app<sup>(123)</sup>.

The standard version of Signal allowed users to link the mobile app to their desktop or other device. The malicious Signal Plus Messenger abused that feature by automatically connecting the compromised device to the IP criminal's Signal in the background, so that all messages were passed onto their account. This happened without the user noticing anything or accepting any notification; it was all done in silence<sup>(124)</sup>. A blog and a YouTube video<sup>(125)</sup> were published on the workings of the attack, claiming that this was the first documented case of spying on a victim's Signal via secret 'autolinking'<sup>(126)</sup>.

Another example of the use of cybersquatting methods on apps is linked to an app called 'Flappy Bird', which was removed from the market in 2014 by its creator. After its removal, IP

<sup>123</sup> Thomas Brewster, Forbes, (2023), [A fake Signal app was planted on Google Play by China-linked hackers](#), accessed on 15 September 2023.

<sup>124</sup> Ibid.

<sup>125</sup> ESETGlobal (YouTube short), [Android users targeted by trojanized Signal and Telegram apps](#), accessed on 15 September 2023.

<sup>126</sup> Stefanko, Lucas (2023), [BadBazaar espionage tool targets android users via trojanized Signal and Telegram apps](#), accessed on 15 September 2023.

criminals created similar apps and inserted malware in order to track users' geolocations, and steal contact list data. McAfee Labs' Threats Report stated that 79 % of the Flappy Birds clones contained malware<sup>(127)</sup>.

Similar apps can also be deceptive in the sense that they use names similar to the original and contain graphics or images that closely resemble those of the original. Two notable versions of Flappy Bird are 'Fly Bird' and 'Flappy Penguin', which used fonts that were almost identical to that of Flappy Bird.

#### V.C.2.d Reverse engineering

To take a legitimate app and create an IP-infringing app, the former can be either altered (changing bytes in compiled source code inside APK, for example), or it can be reverse-engineered to recreate the app functionality with extensive changes. Several tools facilitate this process, including, inter alia, Android Package Kit (APK) tools and Android Studio with emulator to run apps. Ultimately, the process requires a certain level of experience and access to specialised tools (see III.A.2.c).

#### V.C.2.e Deceptive advertising techniques in apps

Malware and fraudulent advertisements can come in many forms. Although they do exist and have been detected in the app space, according to experts in the field, the volumes and proportion of advertising fraud in app advertising are significantly lower compared to that found on websites. Some advertisements promote the download of software that is purportedly needed to fix app issues, upgrade systems, or just to continue viewing content, which could be categorised as system fraud. These advertisements then start the process of installing malware on the user's device, either by directing them to a malicious website or by downloading unwanted or harmful software<sup>(128)</sup>. In the case of apps, these will sometimes appear to the user as an additional update to the app that can be downloaded.

IP criminals – like many who rely on cheap advertisements to make money – likely include misleading and fraudulent techniques to maximise ad revenue.

Advertising format in apps: generally, in apps, the advertisement is either a floating advertisement (equivalent to a static image), or an interactive advertisement<sup>(129)</sup>, which is mostly seen on apps rather than websites.

In apps, there is a significant amount of interactive advertising, unlike what is detected on various websites (mostly IP-infringing websites). Website advertisements may be displayed as images. On the contrary, in IP-infringing apps, the advertisements have video advertising and sometimes even pre-roll videos as advertisements. These allow the users to engage, giving them a small amount of time where they can play a game or interact with something.

---

<sup>127</sup> Dara Kerr (2014), [Flappy Birds clones attract mobile malware at rapid rate](#), accessed on 26 March 2023.

<sup>128</sup> White Bullet / EUIPO (2016), [Digital Advertising on Suspected Infringing Websites](#).

<sup>129</sup> Interactive ads can be a video that is played, or an interactive game that allows playback for a limited time.

App advertisements induce the user to click on them, taking them to a location where they can buy whatever the business is offering.

Due to their interactive qualities, the advertisements are more developed and usually more expensive to create, maintaining a different profile for the apps themselves. If an app operator is earning significant revenue from valuable ad space sales, they may be less likely to deploy other techniques to increase revenues. Other forms of increasing revenues have previously been ad stacking<sup>(130)</sup> or pixel stuffing<sup>(131)</sup>.

*Applying the 'follow the Pixel' strategy has exposed whole new fraudulent advertisement-based scams. In the physical world, what you see is what you get, but in the digital world it is not necessarily so. Therefore, the mind of the investigators has to go beyond what they see because, with data, everything can be disguised.*

IP crime expert

A new initiative was launched partly aimed at combatting the issue of brands unintentionally advertising on pirate sites and apps. To do so, an organisation was established, with the support of tech giants, in an attempt to promote brand integrity and defund pirate sites<sup>(132)</sup>, ultimately protecting advertisers from negative associations. One of its functions includes developing a new blocklist that combines pirate site data with information from anti-malware vendors to also address the issue of advertising<sup>(133)</sup>.

When committing advertising fraud in apps, IP criminals may use techniques similar to those applied on websites to confuse consumers, getting them to click on advertisements and forcing them to give up details, hand over information, and fill in forms. However, it should be noted that the app space is still developing and may still differ as to the presence of malvertising.

The difference between ad fraud on websites and on apps is the landing pages to which the user is taken. In apps, the landing page usually takes the user to download a different app. The techniques are largely the same, but what the user is coerced to do is different.

One example of an app-related advertising fraud case is the following. In 2023, 43 apps distributed on Google Play were found to be engaging in a concerning practice<sup>(134)</sup>. The apps were collectively downloaded 2.5 million times. While the device's screen is off, these apps would load advertisements which is against the Google Play Developer guidelines on how

<sup>130</sup> [Ad Stacking](#) consists of layering advertisements in a single placement so that only the advertisement on the top is visible to the user, while still charging the advertiser fully for the others. Accessed on 26 March 2023.

<sup>131</sup> [Pixel stuffing](#) consists of hiding tiny Ad Spaces, 1x1 pixels in size, and hiding them at the top or bottom of webpages or apps. Accessed on 26 March 2023.

<sup>132</sup> This referenced initiative was established by Trust Accountability Group (TAG) with the support of a few partnering tech giants. For list of partners and information about the TAG initiative, see <https://www.tagtoday.net/>.  
<sup>133</sup> Maxwell, Andy (2024), '[Pirate Sites with Malicious Ads Face Restrictions Under New Initiative](#)', accessed on 19 March 2024.

<sup>134</sup> SangRyu, McAfee (2023), '[Invisible Adware: Unveiling Ad Fraud Targeting Android Users](#)', accessed on 12 January 2024.



advertisements can be displayed. This has an impact on the advertisers who pay for their unseen ads, and on consumers, as it drains batteries, consumes data, poses security threats such as information leaks. Additionally, users must be aware of the implications of granting permissions in apps, such as excluding ‘power saving’ and allowing ‘draw over other apps’. These permissions may allow operations to take place quietly in the background, raising concerns about the motives and actions of the apps or libraries in question. Granting these permissions may lead to more harmful activity, like the display of phishing pages and background advertising.

In the case of click fraud, app techniques are very different to website techniques. For example, pixel stuffing and ad stacking are very specific to websites, because criminals can add them in easily, whereas it is harder to apply them in apps. In the latter case, it is more about the advertisement itself being displayed to the user in the same format as a legitimate ad; rather than from a brand, however, it originates from an IP criminal.

#### V.C.2.f Phishing and ransomware attacks

As more individuals use smartphones and other devices to access the internet, phishing and ransomware attacks on apps are growing more frequent. By impersonating a trustworthy business, phishing attacks attempt to deceive users into disclosing their personal information, such as login credentials or credit card numbers<sup>(135)</sup>. On the other hand, ransomware attacks are a type of malware that encrypts user data and demands money to decrypt it<sup>(136)</sup>.

Phishing or ransomware attacks can take many forms, such as IP-infringing apps imitating financial tools, which is what happened with the IP-infringing Trezor App<sup>(137)</sup>. Trezor was a hardware wallet that secures cryptocurrency assets offline<sup>(138)</sup>. In 2021, in a social engineering scam, IP criminals sent misleading emails to Trezor users from the company’s email address, asking them to click on a link to a trojan horse that was designed to look like the Trezor app and alert them to a ‘data breach’ that had compromised their account. Since the app could be downloaded through major app stores, it was made more believable. As such, many users

*The main challenge is that high-tech criminals usually have a lot of knowledge and experience as well as access to advanced tools, so we therefore need skilled law enforcement investigators and prosecutors who understand these crimes. In order to be able to investigate, they need to have in-depth knowledge of how the cybertechnologies function.*

IP crime expert

<sup>135</sup> Mimecast (2023), ‘[What is Phishing?](#)’, accessed on 26 March 2023.

<sup>136</sup> Check Point (2023). ‘[What is Ransomware](#)’, accessed on 26 March 2023.

<sup>137</sup> David Thomas, Andrew Rossow (2022), ‘[Class-Action Lawsuit Filed Against Intuit for Trezor Phishing Scam](#)’, accessed on 26 March 2023.

<sup>138</sup> [Trezor](#) (2023), accessed on 26 March 2023.

fell victim to these scams and clicked the link, downloading the ransomware or corrupt files onto their devices.

The fraudulent message read as follows:

*Dear Customer,*

*We regret to inform you that Trezor has experienced a security incident involving data belonging to 106,856 of our customers, and that the wallet associated with your email address ... is within those affected by the breach.*

*Namely, on Saturday, April 2nd, 2022, our security team discovered that one of the Trezor Suite and administrative servers had been accessed by an unauthorized malicious actor.*

*At this moment, it's technically impossible to accurately assess the scope of the data breach. Due to these circumstances, if you've recently accessed your wallet using Trezor Suite, we must assume that your cryptocurrency assets are at risk of being stolen.*

*In the spirit of transparency, we wanted to make our customers aware of this incident before malicious actors could utilize this information to their detriment. We felt time was of the essence, and we are expediently working through our investigation.*

*If you're receiving this e-mail, it's because you've been affected by the breach. In order to protect your assets, please download the latest version of Trezor Suite and follow the instructions to set up a new PIN for your wallet.*

Instead of taking customers to the official [www.trezor.io](https://www.trezor.io) landing page, when they clicked the link, they were instead taken to <https://suite.trezor.com>. The app's features were almost identical to the original app; some users did not recognise the little dot under the 'e' character in the fraudulent link.

Trezor tweeted a warning through their main account about the IP-infringing app. After this attack, people were reported to have lost more than USD 1 million dollars' worth of cryptocurrency just by putting their credentials into the app<sup>(139)</sup>.

---

<sup>139</sup> Malwarebytes Labs (2021), [Fake Trezor app steals more than \\$1 million worth of crypto coins](#), accessed on 27 March 2023.

Item 48. Law enforcement investigative strategies relevant  
to IP infringement for malicious and fraudulent purposes

**Law enforcement investigative strategies relevant to  
infringing business model 3**

When law enforcement authorities are investigating an app that is suspected of infringing IP for malicious and fraudulent purposes, there are at least two strategies that may be implemented as part of the investigation.



First, to **follow the pattern**, which entails finding correlations between individual occurrences to begin disclosing clusters of the operation until the full scope is revealed. In some cases, an infringing app operation may seem isolated from other operations, but investigating the infrastructure, ownership and money flow of the operation may reveal connections between several apps and IP criminals. Some investigative techniques involved in 'follow the pattern' include, but are not limited to, the use of internet investigations (e.g., open-source intelligence (OSINT), and obtaining data from internet intermediaries).

Second, the **follow the money** strategy, which involves identifying the infrastructure related to money inflow, identifying the persons involved, and disrupting the money flow. Doing so will also require understanding the tools used to obtain money, whether through electronic, cryptocurrency or traditional bank mechanisms. Following the money may also entail retrieving evidence related to payments and supporting future money-laundering charges.



Read more about business models related to IP infringement carried out for fraudulent and malicious purposes in the infringing business model series <sup>(140)</sup>.

V.C.3 *Criminal gain*

In terms of criminal gain, and as touched upon previously in this report, IP criminals have numerous ways in which to generate revenue through apps. Regarding fraudulent apps, the main channels that IP criminals use to generate income are the following.

- Advertising revenue: IP-infringing fraudulent apps can also incorporate advertisements in order to generate revenue, displaying different types of advertisements to users. Some recurring advertising revenue methods that these IP criminals implement are the integration of malware and fraudulent advertisements such as pixel stuffing or ad stacking.
- Subscription revenue: apps with fraudulent motives can also charge a subscription fee. These types of apps might trick the user into thinking that the app is legitimate and

<sup>140</sup> In the [IBM phase 5](#) report chapter 7, there is a description and analyses of various cybercrimes related to IP. In the [IBM phase 3](#) report, there is a description on how IPTV maliciously disseminated to consumers.

impose a subscription payment. Afterwards, the sensitive payment or personal information that the user provides might be used for fraudulent purposes.

- IP-infringing fraud revenue: for apps that infringe IP, fraud revenue is a less frequent but nonetheless feasible source of income. An app with malware, for instance, might be used to hack a user's device and steal their financial or personal data. Moreover, cryptocurrencies are used by some IP criminals in charging their customers, which could potentially be used for money-laundering purposes.
- Cryptojacking: a technique used by cybercriminals to steal cryptocurrencies from users' wallets and to mine for cryptocurrencies, without bearing the high costs of mining. The ultimate purpose is financial gain. By hacking into devices and installing cryptojacking software, or developing apps with cryptojacking software, cybercriminals are able to run these programs in the background often undetected as users may not notice their devices' slowed performance and lags <sup>(141)</sup> (see also V.C.3).  
*Apps vary depending on how they are being used to make money. For most apps related to IP crime, the ultimate purpose is monetisation, either from mining cryptocurrency from the apps, stealing data from the users that can be later be sold on the dark web, or asking for a subscription or a one-time payment to activate the app.*  
IP crime expert
- One-time fee to download and install an app: developers use this method as a legitimate and common pricing model to generate income. In order to access all of the app's features and functionalities, users must pay a fixed fee, typically at the time of download. However, IP criminals might use this method to trick the user by charging a one-time fee to download the app and then offering an app with no functionality whatsoever.
- Sales revenue for non-delivery: the revenue collected from consumers prior to the expected 'delivery' of the good or service is ultimately the IP criminal's financial gain, and in some cases, the revenue is collected even when the goods or services are not delivered (see IV.C.3)
- Trade secret theft: although the value of trade secrets may vary depending on the sector and the information itself, IP criminals can generate revenue from selling proprietary information, whether through traditional channels or on the dark web (see VI.C.3).

---

<sup>141</sup> Iglezakis, Ioannis (2020), 'Legal Issues Mobile Apps: A Practical Guide'.

## Item 49. Important emerging trend – cryptocurrencies

### Important emerging trend: cryptocurrencies



Cryptocurrencies are a decentralised form of digital money that do not require the verification and settlement procedures of traditional banking institutions. They are decentralised assets administered by way of blockchain technology. Use of cryptocurrencies include payment for purchased goods or services, transfer of value and as investment. The structure of cryptocurrencies usually provides a certain layer of identity obfuscation which, if misused by IP criminals, can pose a challenge for law enforcement and other investigators when monitoring, tracking, and investigating illegal activities involving cryptocurrency transactions. As such, although traditional forms of payment are still common in IP crime, cryptocurrencies have grown in popularity among IP criminals as a means of receiving direct payments, sharing of gain, money laundering and financing IP-related crimes.

Money laundering facilitated by cryptocurrencies entails the passing-off of the proceeds of unlawful activity as legitimate money<sup>(142)</sup>. Since cryptocurrencies can be used to purchase a variety of goods and services, laundered money can be spent without the need to re-enter the traditional financial system. If needing to change cryptocurrencies into traditional currencies, cryptocurrency exchanges are usually applied, and exchanges will normally hold important information about the identity of the cryptocurrency user.

Additionally, cryptojacking is a technique now employed by cybercriminals to reap the benefits of cryptocurrency mining without bearing the high costs of the mining. To do so, cybercriminals hack into devices to install cryptojacking software, or develop apps with cryptojacking software, and users are subject to slower device performance and lags while the app or software mines for cryptocurrencies and steals from cryptowallets in the background<sup>(143)</sup>. To disseminate cryptojacking apps, cybercriminals take advantage of app stores, app marketplaces as well as direct download and other channels of app dissemination to entice users into downloading by promising other functionalities such as computer and battery optimisation, internet search, web browsers, and video viewing<sup>(144)</sup>.

## VI Infringing business model 4: trade secret theft



Many companies develop innovative and ground-breaking technological solutions and therefore rely heavily on the protection of their commercial secrets and practices. It is a priority for the EU to ensure all firms can maintain their competitive advantage, especially those that are technology-focused, driving innovation and continuously aiming to be at the forefront of business development. Trade secrets allow their holder to protect a mechanism or knowledge that cannot be protected under traditional IP rights such as patents, trade marks, or copyright<sup>(145)</sup>; as such, collaboration and cross-border cooperation is particularly important

<sup>142</sup> Financial Crimes Enforcement Network (2023), [What is Money Laundering?](#), accessed on 27 March 2023.

<sup>143</sup> Iglezakis, Ioannis (2020), 'Legal Issues Mobile Apps: A Practical Guide'.

<sup>144</sup> Guo, Yuanjing; Dong, Tommy (2019), '[Several Cryptojacking Apps found on Microsoft Store](#)', accessed on 18 March 2024.

<sup>145</sup> EUIPO '[Study on Business Models Infringing Intellectual Property – Phase 5: Modus Operandi of Serious and Organised Crime](#)'.

in protecting against trade secret theft and thereby protecting innovation<sup>(146)</sup>. Trade secrets can take many forms and are increasingly important to business operations; this section will detail the ways that they may be infringed through IP-infringing apps.

Trade secret theft can occur regardless of whether the parties have a contractual relationship. A common type of trade secrets involves employees or other insiders in the company<sup>(147)</sup>.

Cyberattacks, unauthorised access, and ransomware attacks have been on the rise in recent years. For businesses of all sizes, the theft of trade secrets through cyber-intrusion is serious threats, since they face a risk of losing their innovations or business concepts when priceless information is taken<sup>(148)</sup>.

Trade secret theft through cyber-intrusion are serious threats which can be facilitated through IP-infringing apps. Cyber-intrusion refers to an electronic scenario where an IP criminal may, without authorisation, automatically jeopardise the integrity, confidentiality, or availability of information within an infrastructure by intruding on an operational system (149). Once the IP criminal has access to the app, they can steal sensitive information or carry out reconnaissance to find out more about the business's operations and steal trade secrets. Which may ultimately result in IP infringement and financial damage to the involved parties, including but not limited to software developers and IP owners.

This kind of IP criminality overlaps with traditional cybercrimes like various cyberattacks<sup>(150)</sup>. Such criminal acts include unauthorised access to a computer system (hacking), illegally remaining in a computer system, interference with a computer system, illegal interception of data, illegal data input, data espionage (illegal data acquisition), illegal data interference, and misuse of certain devices.

Trade secrets are of utmost relevance and can be stolen not only by external individuals or IP criminals, but also by insiders from the company victimised by the crime. Therefore, entities are investing more resources into specific tools that protect their trade secrets and maintain their competitive position. Tools such as data loss protection (DLP) technologies, which are designed to detect and prevent unauthorised access and transmission of sensitive information outside the corporate network, are crucial components for information security in any enterprise. The technology works by monitoring and blocking the movement of critical data according to organisational policies on data security and compliance. In this business model, industrial and government espionage is a common practice. It consists of the covert, and sometimes illegal, practice of investigating competitors in order to obtain a competitive advantage<sup>(151)</sup>. Targets in this technique might be trade secrets pertaining to proprietary product specifications or formulae, or information about business plans.

---

<sup>146</sup> Read more about the EU's efforts in protecting trade secrets in [Directive 2016/943](#) on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

<sup>147</sup> See examples from court practice in EUIPO (2023), [Trade Secret Litigation Trends in the EU](#).

<sup>148</sup> European Commission (2022), [New Guide: Cybercrimes and Trade Secret Protection in the EU & China](#), accessed on 25 June 2023.

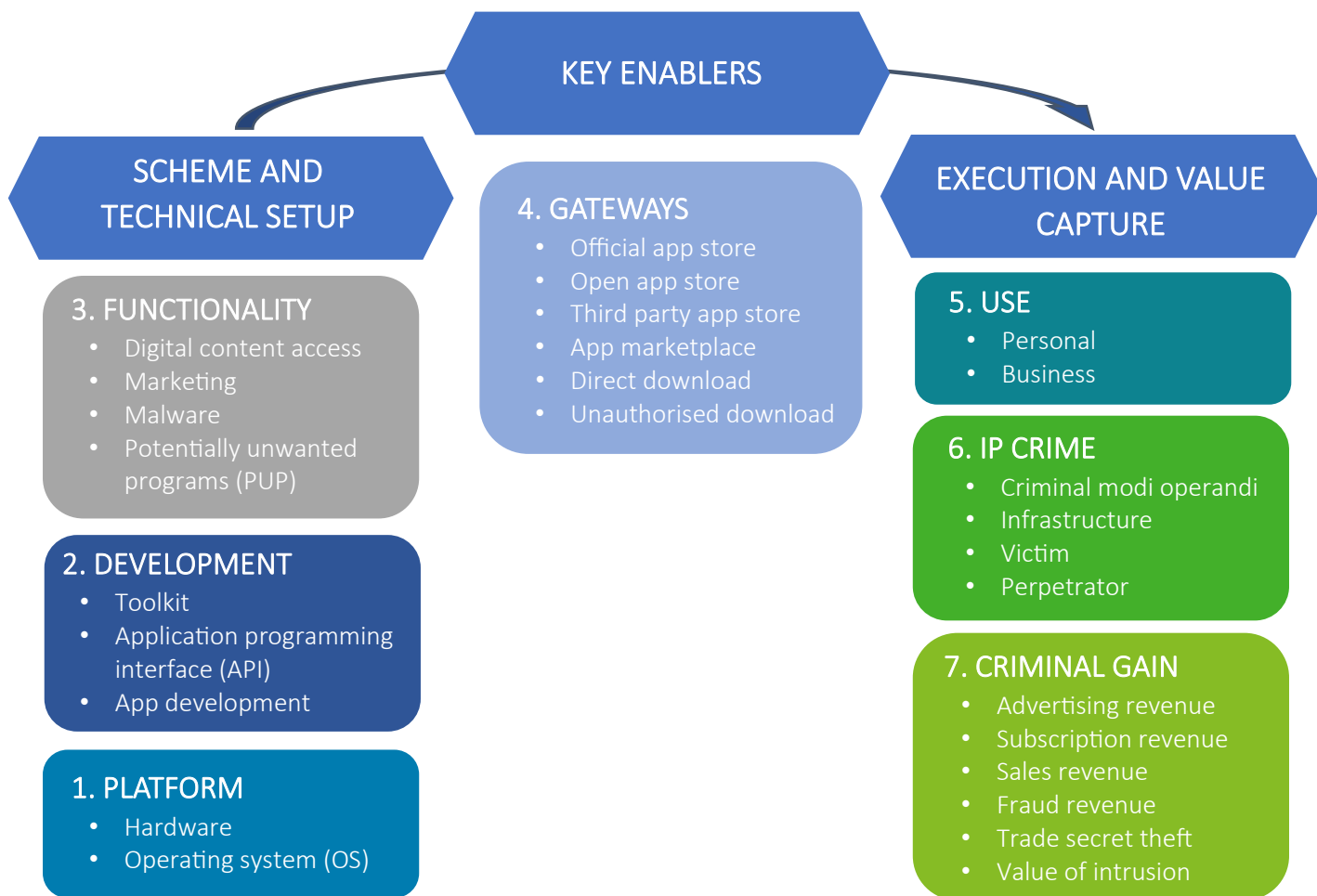
<sup>149</sup> Cornell Law (2023), [Cyber intrusion](#), accessed on 30 March 2023.

<sup>150</sup> See footnote 20 on the EMPACT priorities.

<sup>151</sup> Mary E. Shacklett, Tech Target (2021), [Industrial Espionage](#), accessed on 14 December 2023.

The description of the business models follows the content of *the arc of IP crime related to apps*. The business models described in relation to trade secret theft has a number of overlaps with business model 3 related to fraudulent and malicious IP crime (see V).

Item 50. *The arc of IP crime related to apps*



VI.A Scheme and technical setup



Infringements related to apps, encompass the emerging trend of theft of trade secrets by way of apps.

## VI.A.1 Platform

Focusing on the platform where theft of trade secrets is committed, apps that contain trade secrets can be found in any digital marketplace.

The platform for IP infringement through trade secrets is the same type of hardware, hardware setup, and operating system (OS) as described in the chapter on infringement of copyright protection digital content (see III.A.1) and the chapter on IP infringement for fraudulent and malicious purposes (see V.A.1).

Cyber-intrusion can target any app's platform exploiting weaknesses in the operating system (OS). Not only can the source code of the app, which contains distinctive algorithms, data structures, and logic, contain trade secrets, but also, the design, the functional integration, proprietary libraries, or particular implementation features give an app competitive advantage when considering trade secrets.

### Item 51. Enforcement and investigative measure – collection and handling of electronic evidence

#### Enforcement and investigative measure: collection and handling of electronic evidence



Electronic evidence is becoming increasingly important in all kinds of IP infringement cases, whether civil or criminal. Electronic evidence can originate from internet investigations; extraction of data from networks and devices such as computers, smartphones, tablets, and any other digital device; disclosure of digitally stored information held by intermediaries such as hosting providers and financial institutions; and any other relevant source.

Some traditionally respected good practices are as follows:

- Maintaining and preserving the “order of volatility” so that the evidence may be used later in court. As such, any actions that would change such data must be avoided.
- The person in charge of the investigation must be both trained and certified to do so and be able to explain their actions involving accessing data on digital devices, as well as explaining the impact of these on any digital evidence used in court.
- The chain of custody must be taken and applied to the digital evidence to record the documentation and keep it secure. If an independent third-party forensic expert examines the processes, they must be able to reach the same conclusion.
- The person in charge of the investigation has overall responsibility for ensuring that these secure principles are respected.

## VI.A.2 Development

The development of IP-infringing apps related to trade secrets is to some extent done in the same way as described in the chapter on infringement of copyright protection digital content (see III.A.2) and the chapter on IP infringement for fraudulent and malicious purposes (see V.A.1).



In some cases, IP criminals can develop an app for the sole purpose of stealing trade secrets, meaning the app would facilitate cyber-intrusion, or hacking, to commit trade secret theft. After which, the trade secrets obtained can be used at the IP criminal's discretion. Alternatively, developers may use proprietary frameworks or libraries that contain useful, stolen trade secrets to develop the app itself. In which case, the trade secrets may have been obtained through hacking or through an inside, whether a former employee, or other party (see VI.C.2).

### VI.A.3 *Functionality*

Apps can either be developed using trade secrets obtained without authorisation, or apps can be used as a means to facilitate trade secret theft.

As such, stolen trade secrets can be used to dictate the functionality of another app in the sense that IP criminals may leverage this confidential knowledge, which could include proprietary algorithms, unique code, or specialised knowledge of user interface design and user experience strategies, to offer a competitive edge in developing an app's particular function. By appropriating such information, offenders can shortcut the research and development phase, quickly deploying an app that mimics or surpasses the functionality of the original software. This not only undermines the initial IP owner but also poses significant risks to market integrity and consumer trust, as these infringing apps may not adhere to the same quality and security standards.

In the alternative case, seemingly legitimate apps can be introduced onto devices, thus compromising them, and granting IP criminals access to confidential proprietary information.

## VI.B Key enablers: gateways



The key enabling gateways providing access to download an app related to trade secret theft are the same as described in the chapter on infringement of copyright protection digital content (see III.A.2).

From an enforcement and investigative perspective, the gateway will usually be of unique importance. App stores and app marketplaces might have in place precautionary, preventive, and proactive measures to avoid apps enabling IP crime, and there will often be different types of evidence available from the gateway, including basic subscriber information, transactional data, involved IP addresses, correspondence, and payment information. Read more about internet investigation in V.C.2.b, and digital evidence in VI.A.1.

There are a number of precautionary measures that are implemented within each gateway to prevent IP criminals enabling IP-infringement through apps (see III.B.1 on cooperation with app developers and app stores).

## VI.C Execution and value capture



Depending on how the app is used and the type of infringement, apps can record and profit from IP infringement in a variety of ways.

### VI.C.1 *Use*

IP-infringing apps may provide users with comparable or identical functionality by copying trade secrets from original apps or cracking the encryption and demanding a ransom in exchange. This IP-infringing app could deceive users into believing it is an original app, potentially damaging the reputation of the original app's owner.

However, the use of trade secret theft extends beyond personal use and into the proprietary information of private businesses. Stolen trade secrets can be used to enhance the competitive advantage of an IP criminal's operations which may ultimately compromise the business's reputation and financial gain.

### VI.C.2 *IP crime*

Trade secrets are crucial elements for ensuring an important or dominant market position, especially in commercial sectors where innovation is key. They are usually highly valuable, confidential knowledge and information that provide businesses with a competitive edge. Many trade secrets are specific only to one industry or a niche and can be contained in different parts of an app (i.e., data used in the app's functionality and the software.).

When someone unlawfully obtains, uses, or divulges such confidential knowledge without the owner's authorisation, trade secret theft has taken place. This theft may take place as a result of theft by an insider or hacking into a company's internal systems. While this IP crime can occur on all technical platforms, apps are becoming an increasing threat given their rapid expansion, and the ease of development.

#### VI.C.2.a *Trade secret theft by an insider*

Obtaining trade secrets through an insider is a way for IP criminals to increase their competitiveness, depending on the use of the trade secret. Trade secret information can be used to develop an IP-infringing app with the same functionalities as an existing app. Thanks to the information disclosed, infringers can ruin the holder's competitive edge by replicating all

or part of its trade secret. When the holder’s business model is largely based on the trade secret, the disclosure can even precipitate its bankruptcy (<sup>152</sup>).

Waymo v Uber is a real-life example of a trade secret theft case: in 2017, Waymo (a subsidiary of Google’s parent company) filed a lawsuit against Uber that became one of the most widely followed trade secret misappropriation cases (<sup>153</sup>). The box below provides a detailed description of the case itself.

#### Item 52. Case example – Waymo v. Uber

### Waymo v. Uber Case

Waymo, a pioneer in autonomous vehicle technology, initiated legal proceedings against Uber, alleging collusion with a former Waymo engineer, referred to here as “A”, who departed in 2016. Following his exit, “A” founded Otto, a new venture in the self-driving car domain, which was swiftly acquired by Uber. Subsequently, Uber appointed “A” to lead its autonomous vehicle division. Waymo contended that upon this acquisition, Uber used approximately 14,000 of its confidential files, which “A” allegedly misappropriated to enhance Uber’s own autonomous vehicle initiatives. These files reportedly contained proprietary designs, circuit board layouts, and sensor technologies, pivotal to Waymo’s offerings, with a particular focus on the sophisticated “light detection and ranging” (LIDAR) systems essential for navigation and obstacle detection in autonomous vehicles.

Waymo’s lawsuit sought USD 1.8 billion in damages, asserting that “A’s” actions had expedited Uber’s autonomous program, furnishing Uber with a significant competitive edge by diminishing both developmental timelines and costs. The complaint charged Uber with capitalising on the illicit acquisition of Waymo’s trade secrets, thus securing an unjust competitive lead in the burgeoning market for driverless cars. The dispute culminated in a settlement where Waymo accepted a 34% equity stake in Uber, valued at approximately USD 244 million. Uber also agreed to abstain from incorporating any of Waymo’s confidential technologies in its autonomous vehicle hardware or software.

The case received a lot of media attention and highlighted how crucial trade secrets protection is to the fiercely competitive technology sector.

The potential losses and risks posed by trade secret theft by an insider underscore the critical imperative to consider comprehensive investigative strategies tailored to address such internal threats effectively.

<sup>152</sup> In the [IBM phase 5](#) report chapter 7, there several examples of trade secret theft by an insider, namely previous employees.

<sup>153</sup> Butzel Attorneys and Counselors (2018), [Waymo v. Uber -- ‘Epic’ Trade Secret Case Involving Autonomous Vehicles Settles for \\$244 Million](#), accessed on 3 July 2023.

Item 53. Law enforcement investigative strategies relevant to trade secret theft

**Law enforcement investigative strategies relevant to  
infringing business model 4**

When law enforcement authorities are investigating trade secret theft by an insider, there are at least two strategies that may be implemented as part of the investigation:



Secondly, the **follow the money** strategy which involves identifying the infrastructure related to money inflow, identifying the persons involved, and disrupting the money flow. Doing so will also require understanding the tools used to obtain money, whether through electronic, cryptocurrency or traditional bank mechanisms. Following the money may also entail retrieving evidence related to payments and support future charges of money laundering.

The **follow the person** strategy focuses on identifying the various IP criminals, their affiliations, identifying how they cooperate and collaborate as an organised crime group. Beyond individuals, this strategy also identifies limited-liability companies, foundations or associations used by IP criminals to facilitate their operation and observes the movement of targeted persons to uncover location of the supply-chain.



VI.C.2.b Trade secret hacking theft

Trade secret theft can also occur as a result of hacking, cyber intrusion or cyberattacking, like phishing, the spread of malware, SQL injections resulting in database information disclosure, and social-engineering or brute-force attacks. In some cases, malicious ransomware can be introduced discretely through seemingly legitimate apps and grant IP criminals unauthorised access to confidential information. In other cases, stolen trade secrets can then be exploited to create another IP-infringing app for financial gain or competitive advantage.

In either case, IP criminals are skilled in avoiding detection when it comes to hacking networks, and many companies' intrusion detection systems are unreceptive to IP criminals' tactics. In some cases, IP criminals can avoid detection by manipulating the traffic stream and stealing trade secrets without being immediately detected<sup>(154)</sup>; essentially, a number of techniques may be employed to successfully hack into computer systems and steal trade secrets<sup>(155)</sup>.

An alternative attack vector that could be used by third party applications, if they are downloaded on company devices, is the misuse of permissions given by the operating system. While companies tend to have strict security protocols and policies to prevent such attacks, there is a possibility that an IP-infringing app could be installed. When installed, the app can request a certain set of granular permissions to access internal hardware or software and access proprietary information.

<sup>154</sup> European Commission (2018), '[The scale and impact of the industrial espionage and theft of trade secrets through cyber](#)', accessed on 12 March, 2024.

<sup>155</sup> In [IBM phase 5](#), section 7 outlines a number of specific techniques that IP criminals may use to commit trade secret theft through hacking/cybercrime.

Trade secret theft in apps can ultimately result in substantial financial harm to the affected company, as they undermine its competitive position and permit rivals or unauthorised parties to profit from their knowledge, making them subject to legal repercussions.

For example, in 2019, an app called CamScanner was involved in a real-life case of cyber-intrusion and trade secret theft<sup>(156)</sup>. The main purpose of this well-known mobile app, which was available for both Android and iOS, was to scan documents with a smartphone camera and turn them into PDF files. With over 100 million downloads alone on the Google Play Store, the app became extremely successful.

In August 2019, security experts from Kaspersky Labs found a malicious module in the CamScanner app that posed a serious risk to user security and privacy: a third-party advertising library that included a Trojan Dropper module had been added to the app during an update.

Without the users' knowledge or permission, this Trojan Dropper module was able to download and run malicious programs on their devices. It could potentially reveal user details and perhaps allow unauthorised access to private data kept on the device. This harmful module was not introduced by the creators of the official CamScanner app, but rather by a breach in the security of their advertising-supported app's infrastructure. The logo is simply black in design, with a mint-green stripe at the bottom; within the black area, a block labelled 'CS' is written in white.

*Investigating IP crime is not a one-size-fits-all process. Tools and resources are needed to fight these crimes, which may make it an unbalanced process for small businesses who do not have the adequate tools necessary.*

IP crime expert

After half a month, the company in charge of the app ensured that the latest version of the app was safe, and that the smartphone version was not affected. They also commented that there was no evidence that the suspicious code, injected by third-party advertising software development kits (SDKs), had caused document leaks; therefore, they confirmed that the files were safe<sup>(157)</sup>. In 2021, the company behind CamScanner declared that the malware service was not affiliated with their services and that their logo and name had been taken by the infringers and marketed to users under the pretext that CamScanner was completely free, which was not the case given that the original CamScanner operated under a freemium model.

<sup>156</sup> Shubham Agarwal (2019), '[CamScanner app found to have malware.](#)', accessed on 3 July 2023.

<sup>157</sup> Shubham Agarwal (2019), '[CamScanner app found to have malware.](#)', accessed on 3 July 2023.

Item 54. Law enforcement investigative strategies relevant to trade secret theft

### Law enforcement investigative strategies relevant to infringing business model 4

When law enforcement authorities are investigating an app that is suspected of facilitating trade secret theft, there are at least two strategies that may be implemented as part of the investigation.



First, to **follow the pattern**, which may lead to connecting individual occurrences of app-facilitated trade secret theft to larger IP crime operations. In this strategy, IP crime clusters can uncover the full scope of the operation. In some cases, an infringing app operation may seem isolated from other operations, but investigating the infrastructure, ownership and money flow of the operation may lead to connections between several apps. Some investigative techniques involved in 'follow the pattern' include, but are not limited to, the use of internet investigations (e.g., open-source intelligence (OSINT), and obtaining data from internet intermediaries).

Second, the **follow the money** strategy, which involves identifying the infrastructure related to money inflow, identifying the persons involved, and disrupting the money flow. Doing so will also require understanding the tools used to obtain money, whether through electronic, cryptocurrency or traditional bank mechanisms. Following the money may also entail retrieving evidence related to payments and supporting future money-laundering charges.



Read more about business models related to trade secret theft in the infringing business model series <sup>(158)</sup>.

#### VI.C.3 Criminal gain

The criminal gain that can be derived from trade secret theft facilitated by apps is largely related to the value of the confidential proprietary information stolen. Trade secrets obtained by an insider or through hacking, such as client lists, software updates, source code, design plans, descriptions of manufacturing processes, and personal data, may be sold online for a significant profit, including on the dark web (see III.A.2).

*Few IP-infringing apps operate in isolation, but rather in an organised and globalised ecosystem of crime with enormous profits.*

IP crime expert

In cases where trade secrets are used to develop a competing IP-infringing app, the financial gain that IP criminals may derive can come from the app's commercial success. As a result, the criminal gain that IP criminals may generate in the other business models are applicable (see III.C.3).

<sup>158</sup> In the [IBM phase 5](#) report chapter 7, there is a description and analyses of trade secret theft.

## VII Perspectives and conclusions

The benefits of apps are clear: they enable companies to expand their customer base, modernise their business processes, and offer users a more customised and user-friendly experience. Additionally, apps have accelerated the digital transformation and have evolved into crucial tools for business, government administration, culture, law enforcement, entertainment, and education.

However, issues with IP infringement have also arisen in parallel with and reflecting the proliferation of apps. IP criminals have progressively evolved their business models and are increasingly aware of how to effectively carry out their illicit activities with as low a risk of detection as possible. They have placed themselves further in the background, involving more and more intermediaries to shield themselves and ensure a higher level of anonymity.

### Infringing business models related to apps

This study has identified four main infringing business models related to applications:



- Copyright-protected digital content is a top priority in fighting IP related crimes. IP criminals are consistently advancing their methods of exploiting this content for criminal gain through apps.

- The marketing of IP-infringing physical goods relies on the production, distribution, and transportation to market of goods through the app. This poses challenges to customers in determining whether or not the product is legitimate.



- Fraudulent schemes are plentiful in apps, taking a variety of shapes; users are put at risk of being deceived by IP criminals. These apps can pose significant safety risks to users, tarnishing the reputations of legitimate apps.

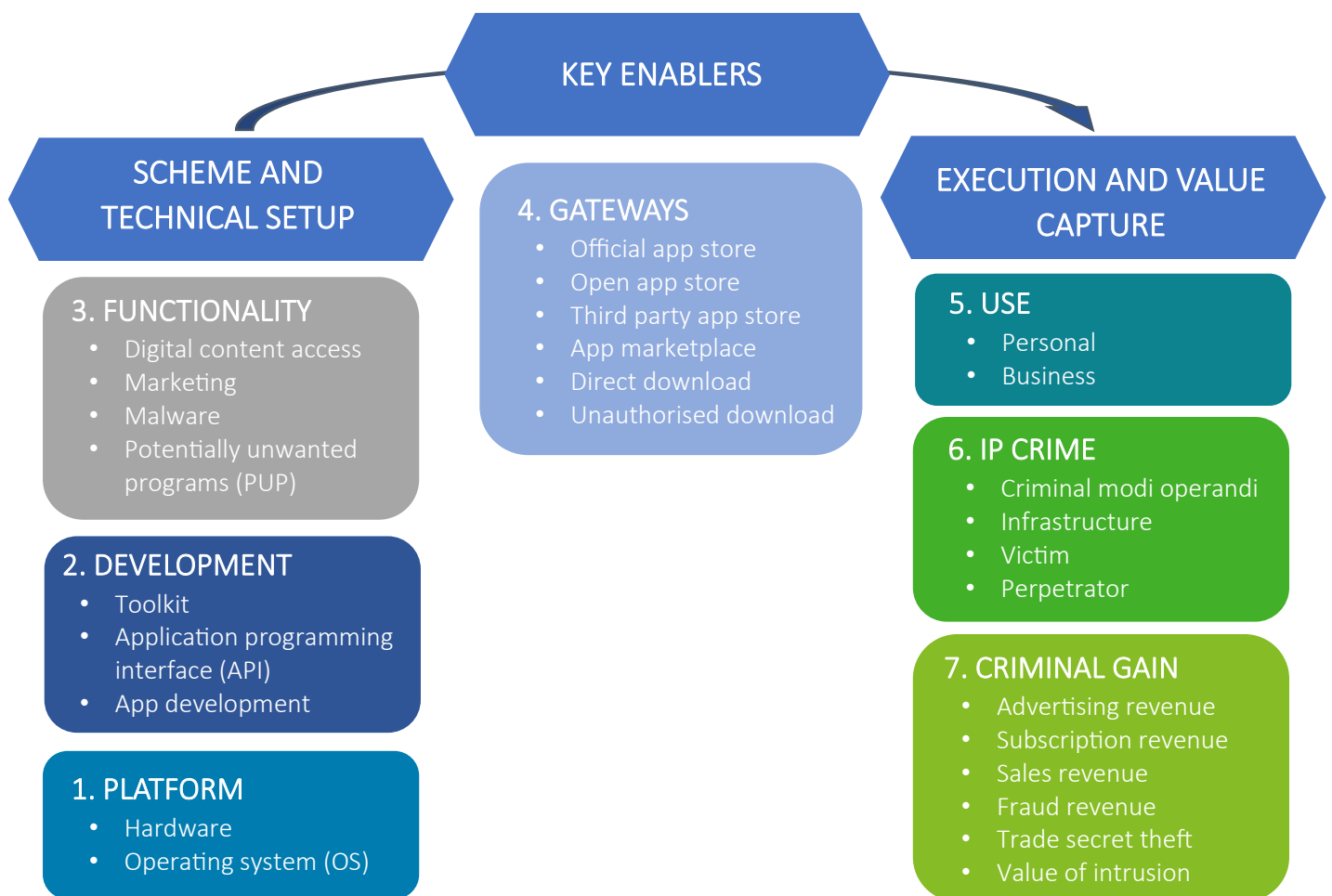
- IP criminals can illegally obtain access to trade secrets using apps or trade secrets to develop their own IP-infringing apps, posing significant risks to both innovation and legitimate apps.



### The arc of IP crime related to apps

Having analysed the various infringing business models found in the app ecosystem, a number of differences and similarities can be highlighted. These include the differentiated model developed for this study, describing the seven main elements of IP crime related to apps.

Item 55. *The arc of IP crime related to apps*



Each of the seven steps is indicative of a particular point within the process of app-related IP infringement. Within the scheme and technical setup of each business model, the platform is the foundation on which the IP-infringing app operates. In deciding on the platform, IP criminals acquire a more enhanced understanding of the requirements for development of the app and its functionality.



To facilitate the particular business model of the IP criminal's operation, the app needs to encompass a number of specific functionalities directly tied to the overall goal of the app. Some of these functionalities are equally applicable in legitimate as well as illicit apps.

Development of apps is increasingly easy and does not always require a deep technical understanding, as several tools exist to facilitate the creation of apps. Development of more complicated apps and functionalities, including intrusion and covert functionalities, might be outsourced to app developers operating covertly (e.g., on the dark web (see )), or through crime-as-a-service (CaaS) (see III.A.2.a) operations.

In the same vein, functionality can be derived from various sources, including for the sole purpose of disseminating copyright-infringing content or marketing IP-infringing goods. In itself, functionality can also be fraudulent, in offering the user nothing in return for the download or payment for goods. Other fraudulent and malicious functionalities include access to and misuse of personal data and dissemination of malware, adware, and other potentially unwanted programs. IP criminals can also determine the functionality of their app by misusing stolen trade secrets from app developers or companies utilising apps, or by creating and using the app to facilitate theft of trade secrets. In any case, functionality can also be altered significantly throughout the lifecycle of an app, allowing IP criminals to change the app's functionalities even after it is approved by app stores and marketplaces, a practice known as versioning (see IV.A.3).

Key enablers are those channels through which IP-infringing apps are disseminated to users; this can be through official app stores, independent platforms, open app stores, app marketplaces, direct downloads, or unauthorised downloads.

To gain from such infringing business models, IP criminals usually alter their behaviour and operations depending on the type of infringement. For copyright-protected digital content, infringement usually entails the dissemination of protected content without the proper authorisation, which can cause financial loss and reputational damage to the IP owner. In the same way, when IP-infringing goods are marketed as legitimate products, the company owning the initial IP may suffer the same damage. This is a damaging practice because users and consumers may be drawn to the IP-infringing goods as a result of their low price point, but they may not expect the lower quality, this harms the overall reputation of the IP owner.

Users and IP owners are usually those who are faced with the most severe consequences as a result of the four business models described above. This is particularly true in the case of the fraudulent business model, which is characterised by IP criminals misrepresenting their apps to users in order to profit. As explained throughout this report, there are several ways in which an IP criminal can achieve this, but ultimately the result is similar: a loss of consumer confidence and the deterrent of app or IP owner's reputation. The fourth business model, involving trade secret theft, yields similar damage, and IP criminals in this case can be IP criminals, cyber-intruders, or former employee's, among others, with the intention of stealing valuable and confidential information to use and facilitate gain.

Therefore, the value captures that IP criminals’ benefit from in disseminating IP-infringing apps can vary depending on the business model. The elements that cause these variations depend on the use of the app, namely whether it is for personal or business use. The criminal gain reaped by IP criminals can derive from various sources, such as advertising, subscriptions, sales, fraud, trade secret value, and intrusion into compromised devices (see below).

A number of emerging threats have been detected, including techniques used in the functionalities of the apps, such as geo-blocking techniques and versioning. The use of dark web (see III.A.2) for development of malicious and fraudulent apps and the sale of trade secrets and the use of social media and encrypted instant messaging and voice over internet protocol (VoIP) apps for communication purposes have also been highlighted. A potential future increased use of superapps (see IV.C.2.c) has also been mentioned. Finally, revenue sources from digital display advertising and the use of cryptocurrency payments have been identified as emerging threats.

To counter app-related IP crime, a number of enforcement and investigative measures, as well as law enforcement investigative strategies, have been developed, used, and enhanced. These include raising awareness among internet users about the threat from fraudulent and malicious apps; cooperation with intermediaries in the app eco-system, including app stores; reverse engineering of apps; deep and comprehensive internet investigations, including cryptocurrency forensics; and careful collection and handling of electronic evidence. Law enforcement authorities also use specialised investigative strategies in IP crime cases, including *follow the goods*, *follow the stream*, *follow the pattern*, *follow the money*, *follow the pixel*, and *follow the person* (see I.C.4).

### **Techniques used for criminal purposes**

For the purpose of review, the following is a criminality table listing the various criminal techniques identified throughout the report, considering the examples of suspected IP-infringing apps.

#### **Item 56. Techniques used for criminal purposes**

<b>Techniques used for criminal purposes</b>	<b>Description</b>
<b>Abuse in lenient jurisdictions</b>	IP criminals occasionally operate in jurisdictions with limited enforcement of IP laws, or other relevant laws, or little participation in international enforcement initiatives. They might exploit this to establish fictitious businesses, entities with no assets or shell companies, or with no physical presence. This makes it challenging to file lawsuits and seek compensation from infringing activities, and unlikely that criminal enforcement measures or investigations will be initiated. They can also benefit from applying bulletproof hosting services or crime-as-a-service (CaaS (see III.A.2.a)).

**RESEARCH ON BUSINESS MODELS INFRINGING  
INTELLECTUAL PROPERTY – PHASE 6: APPLICATIONS  
RELATED TO SERIOUS AND ORGANISED  
INTELLECTUAL PROPERTY CRIME**

<b>Abuse with media players</b>	<p>Media player configurations can be used to access illegal content streaming. Two types of abuse can occur with media players.</p> <ul style="list-style-type: none"> <li>• Generic media players: third-party developers can create add-ons and plugins in legitimate media players allowing users to access copyrighted material.</li> <li>• Infringing media players: this can be the case for content delivery network (CDN) abuse, where apps work their way around digital rights management (DRM) to provide unlawful access to copyrighted content.</li> </ul>
<b>Unsecure distribution and installation of Android package kits (APK)</b>	<p>APK files are plentiful on the internet and can be drawn from a number of legitimate, as well as illegitimate, sources. In cases where IP criminals upload their apps to official marketplaces in the form of APK files, it can be difficult to ensure that the apps come from trustworthy sources. When the distribution channel may be untrustworthy, these apps might include malware, spyware or scraping functions that collect personal information from the user's phone without the user finding out or authorising it.</p>
<b>Anonymisation</b>	<p>In this technique, IP criminals operating apps may hide their identity under several layers of obfuscation techniques. This strategy makes it difficult for IP owners and law enforcement to identify and investigate the IP criminals.</p>
<b>Application programming interface (API) abuse</b>	<p>APIs make it simpler for developers to create software apps, for example, communicating with other services. If an API is used incorrectly, it may result in IP infringements, such as the illegal use of another party's confidential information as well as copyrighted or trade-marked content.</p>
<b>Blocking the screenshot functionality</b>	<p>IP criminals sometimes restrict users from taking screenshots while using the app, making it more difficult to detect and report infringement.</p>
<b>Brand abuse or brand impersonation</b>	<p>Infringing businesses imitate original brands in order to deceive user into believing that they are either at the real website/app or an associated page of the genuine brand. They extensively replicate brand trade marks, website/app design, product listings, and other elements.</p>
<b>Camouflage techniques</b>	<p>IP criminals can create apps that appear to come from a trustworthy brand with the aim of tricking the internet user into downloading the app. Subsequently, these apps might infect the device and operate covertly without users' knowledge, stealing sensitive information, and other unwarranted actions.</p>
<b>Circumventing regulations in app stores and marketplaces</b>	<p>Some IP-infringing apps bypass the measures put in place by app stores and marketplace operators to prevent, detect and remove illegal apps by providing direct downloads or making the apps available through other alternative measures. See also about versioning in IV.A.3.</p>
<b>Cryptojacking</b>	<p>Cryptojacking is a form of cybercrime that involves the unauthorised use of people's devices to mine for cryptocurrency. The ultimate purpose is for cybercriminals to benefit from cryptocurrencies without bearing the high costs of mining. Cybercriminals hack into devices to install cryptojacking software, or develop apps with cryptojacking software, and users are subject to slower device performance and lags while the app or software mines for cryptocurrencies and steals from cryptowallets in the background.</p>
<b>Error! Reference source not found. Disguising techniques</b>	<p>IP criminals sometimes might disguise where they are sourcing the copyright-infringing content from, within their apps, and ensure that the app closely resembles a legitimate streaming service, like music streaming services.</p>

**RESEARCH ON BUSINESS MODELS INFRINGING  
INTELLECTUAL PROPERTY – PHASE 6: APPLICATIONS  
RELATED TO SERIOUS AND ORGANISED  
INTELLECTUAL PROPERTY CRIME**

<b>Domain Name System (DNS) abuse</b>	Although cybersecurity standards are improving, as apps can gather private user information, domain name system (DNS) abusers are drawn to them, which might result in data breaches, financial loss and reputational damage. DNS abuse can be seen in cybersquatting and typosquatting. This resembles the malicious and fraudulent misuse of a trade mark in an app name (also known as app squatting).
<b>Geo-blocking techniques</b>	Applied by IP criminals, where infringing content is only shown in targeted countries, as an obfuscation technique. IP criminals would then block the use of VPNs as well and/or use an emulator.  Example: case of a provider in that makes sure the app is not available in their country of residence, but only where the target audience is located.
<b>Payment circumventing techniques</b>	Subscription methods are easily tracked by law enforcement, and yet IP criminals have created new ways to charge their users. In order to hide where the money is going, when making the payment, some apps state that the charge will appear on the user's statement under another name, blinding law enforcement officers to these infringing movements.
<b>Subscription based illegal IPTV techniques</b>	Subscription-based illegal IPTV is more present than the abovementioned technique. With this methodology, IP criminals decide who they let onto their platform by making the user pay a subscription fee. They facilitate illicit online dissemination of copyright-protected content.
<b>Terms and conditions (T&amp;C) manipulation</b>	IP criminals engage in misleading activities seeking to deceive users and authorities about who really owns and controls the app, as well as the direct liabilities and terms tied to the app, making it more difficult to enforce IP protection. Moreover, T&Cs can be altered to resemble those of legitimate apps, with minor modifications, giving users the illusion that the app is legitimate and trustworthy. Ultimately, IP criminals may illicitly put different entities in their terms and conditions (T&C) by adding erroneous information or different businesses.
<b>Traditional P2P filesharing techniques</b>	This criminal technique is no longer that frequent, but it is still present. It is commonly used to download or watch copyrighted material and facilitates illicit online dissemination of copyright-protected content.
<b>Versioning</b>	IP criminals may change the functionality of their apps after the app is approved by official app stores or marketplaces, as a means to bypass the screening procedure and regulations. Information on how to modify an app's functionality can be found in different platforms, usually online forums, where users share information. As official app stores and marketplaces implement their screening procedures before publishing the app on their platforms, and often times whenever there is an update, normally the altered version of the app will be found in other app stores. Essentially, once the correct version is downloaded from that external marketplace, the IP-infringing content can be accessed.

## Revenue sources

IP criminals may derive value through a number of sources related to apps. The main channels that IP criminals use to generate income are the following.

### Item 57. Revenue sources

Revenue sources	Description
<b>Advertising revenue</b>	If an app infringes IP, the app developer may be making money from advertisements that are shown next to the infringing content. Advertisements may be visible or hidden, include legitimate advertising or fraudulent advertising, and may be benign or harmful or bothersome to the user.
<b>Compromised device value</b>	Another potential method of illicit gain for apps violating IP laws is intrusion, compromising a user's device, or trade secret theft. An app with malware could be used to access a user's device without authorisation, giving IP criminals access to trade secrets or sensitive information.
<b>Data theft</b>	Cyber-intrusions can be used to steal user data, including payment and personal information, which can then be sold on the dark web or used for financial advantage.
<b>Fraud revenue</b>	An app with malware, for instance, might be used to hack a user's device and steal their financial or personal data. Cryptocurrencies are also increasingly being used by IP criminals in charging their users, which could potentially be used for money laundering purposes. Ad fraud is another mechanism that allows IP criminals to charge advertisers without showing their ads to users in the manner agreed upon.
<b>One-time fee fraud</b>	In order to access all of the app's features and functionalities, users must pay a set fee, typically at the time of downloading and installing the app. However, IP criminals might use this method to trick the user by charging a one-time fee to download the app and then encountering themselves with a blank app with no functionality whatsoever.
<b>Sales revenue</b>	An app that offers users illegal music or films can make money from the sale of that content.
<b>Subscription revenue</b>	To access premium features or content, some apps charge a fee to users. If an app infringes the IP of others, the developer may be making money from subscription fees for access to the content.
<b>Trade secret value</b>	A trade secret will not only have value to the company to which it belongs, but it can be monetised by extortion or sale, or it can be directly misused by a recipient.

## **Enforcement and investigation**

App creators may proactively protect their IP, including registering app names and logos as trade marks. They might also rely on copyright protection of the source code of their apps. By safeguarding and relying on IP, developers can prevent possible IP infringements and ensure legal consequences in the event of infringement.

To combat such crimes, various measures need to be in place, and it is of utmost importance to raise awareness among internet users about the dangers of being misled by apps to access fraudulent online services and schemes. Moreover, cooperation between digital marketplaces, IP owners, and developers is crucial, as is the implementation of tight criteria and review procedures, the timely removal of illegal apps, and assistance for IP enforcement operations.

Investigators can also employ reverse engineering to dissect and scrutinise the internal workings, functionalities, and security features of an app. This technique allows the modus operandi of the criminal activity to be better understood. Usually referred to as the ‘follow the pattern investigative strategy’, what appear to be separate and isolated digital phenomena can be seen as part of the activities of the same criminal group and can disclose the true scope of the enterprise.

Another investigative technique falls under the scope of open-source intelligence (OSINT) and entails the gathering of information, intelligence, data and/or evidence from open sources. Known as live internet investigations, information collected in this way can be used as intelligence, be actionable, and be used as evidence in a court of law. Unlike traditional intelligence-gathering methods, which can often rely on classified sources, OSINT focuses on procuring information from sources accessible to the general public; a special area of OSINT is social media intelligence, also known as SOCMINT, which extracts intelligence from social media platforms.

In the same vein, electronic evidence is becoming increasingly important, especially in cases related to IP-infringing apps. In addition to live internet investigations, this evidence can be obtained through the extraction of data from networks and devices and disclosure of digitally stored information held by intermediaries. An effective investigation relying on these methods requires significant cooperation between law enforcement authorities, the intermediaries – namely app stores and official marketplaces – and IP owners.

Item 58. **Enforcement and investigative approaches**

Enforcement and investigative approaches	Description
Copyright infringements online	When law enforcement investigates online copyright infringements related to apps, special attention can be paid to disclosing as much of the network as possible, detecting correlations between websites, apps, and any other digital phenomena. This will always require internet investigation and usually also a financial investigation. To support the investigation, reverse engineering of the apps and obtaining evidence from intermediaries will often be relevant.
Fraud	When law enforcement investigates online app-related fraud, special attention can be paid to disclosing connected fraudulent websites, social media accounts and other means used to defraud internet users. This will always require internet investigation and usually also a financial investigation. Careful attention to securing volatile digital evidence will often be decisive to be successful. Criminal investigations and prosecutions can be used to raise the awareness among the general public of measures to avoid fraud.
Malware dissemination	When law enforcement investigates malware dissemination related to apps, internet investigation, careful collection of volatile electronic evidence and often also a financial investigation will be necessary. Reverse engineering will often be an effective means of investigation. Criminal investigations and prosecutions can be used to raise the awareness in the general public about measures to avoid malware infections.
Marketing of IP-infringing physical goods	When law enforcement investigates marketing of IP-infringing goods related to apps, special attention can be paid to detecting correlations between vendor on e-commerce platforms, websites, apps and any other digital phenomena. This will often require internet investigation, financial investigation; if possible, it can also be effective to try to disclose the full supply chain of the IP-infringing goods. To support the investigation, reverse engineering of the apps and obtaining evidence from intermediaries will often be relevant.
Trade secret hacking theft	When law enforcement investigates app-related trade secret hacking theft, internet investigation and collection of volatile electronic evidence will always be necessary. Criminal investigations and prosecutions can be used to raise awareness among companies (especially small and medium-sized companies) about measures to avoid hacking.
Trade secret theft by insider	When law enforcement investigates trade secret theft by an insider, it will often be necessary to apply a 'follow the person' strategy involving observation and surveillance. As the trade secrets will usually be in electronic form, comparison of large amounts of data will often be required.

This report was developed in parallel with the Multi-disciplinary Platform against Criminal Threats (EMPACT) framework, a security initiative driven by EU Member States to identify, prioritise and address threats posed by serious and organised international crime, where IP crime is a dedicated priority (see footnote 20).

The report documents the need for a robust criminal enforcement response to serious and organised IP crime, which is also in line with the recent Commission recommendations to combat counterfeiting and protect IP (see footnote 21), which included a number of actions that can improve the criminal enforcement response to IP crime.

Serious and organised criminals recognise the value of IP and may seek to exploit it through different avenues of IP crime as illustrated in the report. When IP owners are confronted with serious, mostly wilful, IP infringement, often on a commercial scale, they may choose to refer the case to a public investigating authority for criminal enforcement (see II.E.1.b). In a report supplementary to this business model study, *the Intellectual Property Owner Guide to Criminal Referrals in Intellectual Property Crime Cases* sets out a roadmap to assist IP owners who choose to refer cases involving the infringement of their respective IP to investigating authorities for criminal enforcement.

As every country will have its own national standards on imposing criminal sanctions for criminal trade mark counterfeiting, criminal copyright infringement, trade secret theft, and other IP-related crimes, the upcoming EUIPO study *Legislative Measures Related to Intellectual Property infringements - Phase 3: Criminal Measures in Serious and Organised Intellectual Property Crime Cases* planned for publication in mid-2024, aims to provide a comprehensive overview of the scope and substance of criminal measures related to IP-related crime in general.





[www.euiipo.europa.eu](http://www.euiipo.europa.eu)

# RESEARCH ON BUSINESS MODELS INFRINGING INTELLECTUAL PROPERTY

Phase 6: Applications Related to Serious and  
Organised Intellectual Property Crime

© European Union Intellectual Property Office, 2024

Reuse is allowed provided the source is acknowledged and changes are mentioned (CC BY 4.0)

