

ILLEGAL IPTV IN THE EUROPEAN UNION

RESEARCH ON ONLINE BUSINESS MODELS INFRINGING INTELLECTUAL PROPERTY RIGHTS — PHASE 3

Report



ILLEGAL IPTV IN THE EUROPEAN UNION

ISBN 978-92-9156-270-1 doi: 10.2814/28041 TB-03-19-764-EN-N

© European Union Intellectual Property Office, 2019

Reproduction is authorised provided the source is acknowledged

Economic, Legal and Technical analysis Report

November 2019

Contents

FOREWORD.....	5
EXECUTIVE SUMMARY	6
1. PROTECTION OF TELEVISION BROADCASTS IN THE EUROPEAN UNION	11
1.1 INTERNATIONAL AND EU LEGAL FRAMEWORK	11
1.2 RIGHTS IN TV BROADCASTS UNDER EU LAW: SUBSISTENCE AND OWNERSHIP... 13	
1.2.1 <i>Copyright protection of broadcast content.....</i>	<i>13</i>
1.2.2 <i>The related right in broadcasts of broadcasting organisations.....</i>	<i>14</i>
1.3 THE SCOPE OF BROADCASTERS' RIGHTS ON THE INTERNET	14
1.3.1 <i>Making available right: on-demand versus live streaming</i>	<i>15</i>
1.3.2 <i>Online remote recording of TV programmes</i>	<i>15</i>
1.4 THE PROTECTION OF BROADCAST CONTENT	16
1.4.1 <i>Reproduction right and the exception for temporary acts of reproduction.....</i>	<i>16</i>
1.4.2 <i>Communication to the public by retransmission of TV signal via the internet</i>	<i>17</i>
1.4.3 <i>Communication to the public by hyperlinking</i>	<i>17</i>
1.5 LEGISLATIVE DEVELOPMENTS: THE NEW DIRECTIVE ON ONLINE BROADCAST TRANSMISSION.....	19
1.5.1 <i>Ancillary online services.....</i>	<i>19</i>
1.5.2 <i>Online retransmission services</i>	<i>20</i>
1.5.3 <i>Direct injection</i>	<i>20</i>
1.6 THE LEGISLATION OF EU MEMBER STATES	20
1.6.1 <i>Subsistence and ownership</i>	<i>21</i>
1.6.2 <i>Scope of the rights: communication to the public</i>	<i>21</i>
1.6.3 <i>Limitations and exceptions.....</i>	<i>23</i>
1.6.4 <i>Legislative developments in Member States.....</i>	<i>23</i>
1.6.5 <i>The protection of sporting events.....</i>	<i>24</i>
1.6.6 <i>Indirect or secondary liability for copyright infringement.....</i>	<i>25</i>
1.6.7 <i>Other legislation potentially covering IPTV infringement</i>	<i>25</i>
2. SUSPECTED COPYRIGHT INFRINGING IPTV ECOSYSTEM.....	26
2.1 BUSINESS MODELS.....	26
2.1.1 <i>Illegal IPTV Subscription.....</i>	<i>26</i>

2.1.2	<i>Illegal IPTV for Resellers</i>	28
2.1.3	<i>Illegal IPTV Free Streaming Portal</i>	29
2.2	THE ACTORS OF THE ILLEGAL IPTV ECOSYSTEM	30
2.3	HOW THE ECOSYSTEM WORKS	31
2.4	INDIVIDUAL ACTORS.....	35
2.4.1	<i>Front-end Actors</i>	36
2.4.2	<i>Back-end Actors</i>	39
3.	QUANTITATIVE ANALYSIS OF SUSPECTED ILLEGAL IPTV IN THE EU	47
3.1	MAGNITUDE OF ILLEGAL IPTV: USERS	48
3.2	MAGNITUDE OF ILLEGAL IPTV: REVENUE	50
3.3	METHODOLOGY AND DATA.....	56
3.3.1	<i>Unauthorised IPTV Users</i>	56
3.3.2	<i>Unauthorised IPTV Revenue</i>	58
4.	ENFORCEMENT MEASURES	62
4.1	THE ROLE OF INTERNET INTERMEDIARIES	62
4.1.1	<i>'Active' intermediaries</i>	63
4.1.2	<i>Hosting services</i>	63
4.1.3	<i>Mere conduit and caching</i>	64
4.2	CIVIL ENFORCEMENT MEASURES	65
4.2.1	<i>Blocking injunctions</i>	65
4.2.2	<i>Dynamic injunctions</i>	66
4.2.3	<i>Live blocking injunctions</i>	66
4.2.4	<i>De-indexing injunctions</i>	66
4.2.5	<i>Disclosure of information</i>	66
4.3	CRIMINAL ENFORCEMENT MEASURES	67
4.4	ADMINISTRATIVE PROCEDURES.....	68
4.5	CUSTOMS MEASURES REGARDING STREAMING DEVICES	69
5.	SELECTED JURISPRUDENCE OF MEMBER STATES	71
5.1	CIVIL CASE LAW AGAINST DIRECT INFRINGERS	71
5.1.1	<i>Standing to sue</i>	71
5.1.2	<i>Retransmission of TV signal via internet live streaming</i>	72

5.1.3	<i>Hyperlinking to infringing IPTV</i>	73
5.1.4	<i>Illicit IPTV devices</i>	75
5.2	INJUNCTIONS AGAINST INTERNET INTERMEDIARIES.....	75
5.2.1	<i>Live blocking injunctions against network providers</i>	76
5.2.2	<i>Injunctions against search engines and social media</i>	77
5.2.3	<i>Injunctions against streaming servers</i>	78
5.2.4	<i>Disclosure of information</i>	79
5.3	CRIMINAL CASE LAW.....	79
5.3.1	<i>Hyperlinking cases in the Czech Republic and France</i>	79
5.3.2	<i>Illicit IPTV and cardsharing in Denmark</i>	80
5.3.3	<i>Illicit IPTV devices in the United Kingdom</i>	81
6.	CONCLUSIONS AND PERSPECTIVES.....	84
	BIBLIOGRAPHY.....	85
	APPENDIX I — REVIEW OF POLICY, ECONOMIC AND TECHNICAL LITERATURE.....	93
I.I	— MAGNITUDE OF ILLEGAL IPTV.....	94
I.II	— USE OF ILLICIT STREAMING DEVICES.....	95
I.III	— IMPACT OF ILLEGAL IPTV.....	96
I.IV	— REVENUE SOURCES.....	97
I.V	— TECHNICAL LITERATURE ON ILLEGAL IPTV.....	99
	APPENDIX II — CASE STUDIES OF INTELLECTUAL PROPERTY RIGHTS’ INFRINGING ONLINE BUSINESS MODELS APPLIED BY UNAUTHORISED IPTV PROVIDERS.....	100
II.I	— ILLEGAL IPTV SUBSCRIPTION ONLINE BUSINESS MODEL (‘IPTV RETAILERS’).....	100
II-II	— ILLEGAL IPTV FOR RESELLERS (‘IPTV WHOLESALERS’).....	101
II-III	— ILLEGAL IPTV FREE STREAMING PORTALS (‘LINK AGGREGATORS’).....	101
	APPENDIX III — ECOSYSTEM OF ILLEGAL IPTV.....	114

FOREWORD

Watching television is part of the modern life, but technology is changing patterns of consumption of news broadcasts, game shows, television series, videos or sports events. This has opened up new opportunities for businesses, and also for the infringement of IP rights.

The television market has experienced a paradigm shift from traditional modes of broadcasting by air, satellite and cable toward internet-based streaming. This is known as IPTV (internet protocol television) and includes live and on-demand streaming of television content online.

IPTV technology offers advantages to legitimate content providers such as flexible online access, time-shifted media and video on demand. This has led to market expansion and an increasing number of subscribers for legitimate services.

However, unauthorised delivery of IPTV content is also on the rise.

While illegal IPTV does not account for the majority of illegal streaming, it is arguably one of the most lucrative areas.

This report estimates EUR 941.7 million of unlawful revenue was generated by copyright infringing IPTV providers in the EU in 2018 and that these services were used by 13.7 million people in the EU (3.6 % of the EU-28 population).

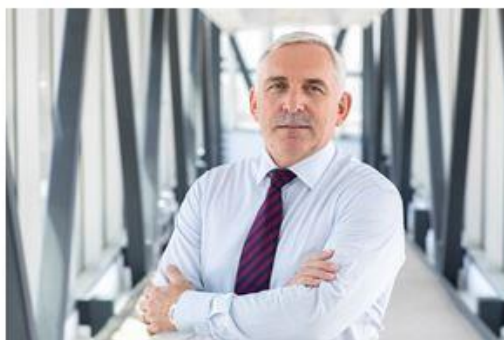
This is a market area in which infringing business models change quickly as they adapt to new technology and business opportunities.

This research clarifies the technology used, the complex supply chains and legal issues.

It also casts much-needed light on a hidden area of an everyday activity, which is being exploited by organised crime, and should help raise awareness among EU citizens.



Christian Archambeau
Executive Director
EUIPO



EXECUTIVE SUMMARY

Background

In 2018, the European Union Intellectual Property Office (EUIPO), through the European Observatory on Infringements of Intellectual Property Rights, commissioned a research study on IPTV crime in Europe. The purpose of the research study was to enhance the level of understanding about the ways illegal internet protocol television (IPTV) is carried out, how the business models around this phenomenon work, and thereby provide a basis for subsequent identification of possible responses to tackle the challenge of the phenomenon more effectively.

The research study was commissioned to the Centre for Intellectual Property Policy and Management (CIPPM) of Bournemouth University, which set up a team of researchers in law, economics and computer science⁽¹⁾. The research team was assisted by an expert group including rights holders, law enforcement representatives, regulatory authorities, civil society groups and digital security companies⁽²⁾.

The present report is carried out as an interdisciplinary study, surveying legal, technical and economic aspects of illegal IPTV. It is the first major study that reviews the existing literature, the legislative framework and case-law in the EU and provides structural analysis of existing business models with regard to unauthorised delivery of television content over the internet. In addition, the study provides the first assessment results of the magnitude of illegal PTV across the EU in terms of active users and unlawful revenue obtained from infringing activities.

Methodology and Data

The existing studies⁽³⁾ aiming to quantify the magnitude and economic impact of illegal IPTV coherently report on the rising trend of unauthorised IPTV proliferation in global markets⁽⁴⁾. This report has been carried out to estimate the number of individuals involved in consumption of unauthorised IPTV as well as to assess the potential revenue generated by copyright infringing IPTV providers. Quantitative estimation is based on official and harmonised data sources in order to ensure full comparability of the reported estimates among the EU Member States. Official Eurostat household survey data was applied when possible. This study also benefits from cooperation with the EUIPO

⁽¹⁾ Bournemouth University research team was led by Professor Maurizio Borghi and included Professor Vasilis Katos, Dr Antanina Garanasvili and Dr Marcella Favale as Principal Investigators, and Professor Dinusha Mendis, Ms Dimitra Poutouri and Mr Dimitris Mallis as Co-Investigators.

⁽²⁾ The expert group included Bogdan Ciinaru (Europol), Tim Cooper (Premier League), Richard Crisp (BT), Callum Cryer (UK IPO), Mattia Epifani (Re@lity Net), Matteo Feraboli (Sky Italia), Jose Luiz Gomez (Spanish Police), Gabor Ivanics (Eurojust), Jerry Gee (Kudelski-Nagra), Phillip Davies (Sky UK), Robert Kiessling (Sky UK), George Kyne (An Garda Siochana), David Lowe (UK IPO), Yuliya Morenets (TAC International), Mark Mulready (Irdeto), Marco Musumeci (UNICRI), Mathilde Persuy (Hadopi), Marco Signorelli (DCP), Laura Vilches (Spanish Liga), Alessandro Rossetti (SoftStrategy), Kevin Taylor (Comcast), Lars Underbjerg (Nordic Content Protection), Didier Wang (Hadopi).

⁽³⁾ Cybersecurity unit of Kudelski Group (2016), Hadopi (2018), Nordic Content Protection (2017), Sandvine (2017), The Industry Trust (2016).

⁽⁴⁾ See *infra* Appendix I.

Observatory stakeholders and relies on data and knowledge shared by experts of IPTV market conditions.

Business models in the unauthorised IPTV market are defined in compliance with the methodology developed by EUIPO 'Research on Online Business Models Infringing Intellectual Property Rights' ⁽⁵⁾. The analysis of the ecosystem of business models of illegal IPTV across the EU includes the applicable legal framework and the significant case-law.

The legislative framework investigation was assisted by a survey carried out in 28 EU Member States. Based on preliminary analysis of the *acquis communautaire* on copyright protection of television broadcasts, a survey of the relevant law and jurisprudence of Member States has been conducted by means of a questionnaire addressed to national correspondents. The survey allowed to collect case law on illegal IPTV, both from civil and criminal proceedings, and to identify the nuances of applicable legislation among national jurisdictions.

Legislative framework analysis

European Union law provides for a broad protection against unauthorised transmission of TV broadcasts on the internet, covering a wide range of activities. Retransmission of air, satellite or cable signal on the internet, cloud recording of TV programmes, hyperlinking to live streaming through smart TV devices and indexation of hyperlinks constitute acts of 'communication to the public' under Article 3 of the Information Society Directive. However, not all rights that subsist in TV broadcasts are protected in the same way across the EU. Rights in the content incorporated in TV broadcasts are protected against both live and on-demand streaming. By contrast, broadcasters' rights in the broadcast signal apply only to on-demand streaming (or downloading) of fixations of broadcasts. Only seven Member States (Austria, Czech Republic, Denmark, Finland, Romania, Sweden and the UK) extend broadcasters' rights to live streaming as well. In addition, reception of TV signal by means of unauthorised streaming devices is an infringement of the reproduction right under Article 2 of the Information Society Directive.

While content incorporated in TV broadcasts enjoys a high level of protection against illegal IPTV, sporting events as such are not a subject matter of copyright protection under EU law. However, audiovisual recording of sporting events is likely to meet the conditions of subsistence of copyright, by virtue of the 'free and creative choices' made by the director of the recording. Moreover, the works and other subject matter normally included in the recording and transmission of sporting events (such as background sound recording, original music and graphic works) are likely to attract copyright too.

The *acquis communautaire* leaves some uncertainty as to whether simultaneous retransmission of free IPTV signal, including by means of framing, and transmission of IPTV signal to a signal distributor by means of 'direct injection' constitute acts of communication to the public under Article 3 of the

⁽⁵⁾ EUIPO 'Research on Online Business Models Infringing Intellectual Property Rights': Phase 1, Establishing an overview of online business models infringing intellectual property rights, July 2016.

Information Society Directive. Both scenarios are addressed by the new Directive on Online Broadcast Transmission (2019/789), which will be implemented in Member States' legislations by June 2021.

Copyright Infringing Business Model Analysis

Copyright infringing IPTV distribution shows a variety of patterns and ranges from well organised large business structures to individual undertakings. While providing the same product, namely access to live streamed channels, illegal IPTV providers vary in terms of the platform on which the access to IPTV is made available, target audience, pricing strategies and other elements such as complementary products (video on demand, set-top box sales) and social media presence. Infringement can simply commence when an unlicensed content provider legally obtains a stream from a content distributor or content provider and makes it available to third parties this way violating the terms of use. These third parties may be end users and consumers of the content, or intermediaries, in which case they may also make profit by reselling it.

Technological developments as the spread of broadband penetration and higher internet speed do not only facilitate access to legitimate IPTV sources, but in turn simplify access to those that are illicit. Technological challenges must be taken into account when considering the impact of illegal IPTV thus adding to the complexity of the analysis. Despite the variety of means of distribution, the analysis shows that illegal IPTV tend to cluster around three broadly defined business models:

- The 'Illegal IPTV subscription' model, where customers are given direct access to a number of TV channels upon subscription and payment of a fee. IPTV content is made available for direct streaming on the illegal websites or through mobile device applications. This business model is based on sale of unauthorised IPTV subscriptions to consumers and revenue is generated from monthly payments collected from subscribers.
- The 'Business-to-business' model. This business model is oriented toward resale of packages of IPTV channels and facilities to set up an illegal IPTV resale. This type of business model can be described as 'business-to-business', or 'wholesale' model. It is frequently combined with the former business model of direct subscription sales. In this case two sources of revenue are guaranteed to unauthorised IPTV providers: monthly payments collected from unauthorised IPTV viewers and payments collected from unauthorised IPTV resellers.
- The 'Streaming portal' model, where links to streaming websites are collected and made available to end-users. IPTV streaming is offered free of charge and frequently in a lower quality compared to subscription-IPTV websites. As the streaming content is provided free of charge, unauthorised providers generate revenue through indirect sources, spreading malware or collecting 'pay-per-view' and 'pay-per-click' payments from advertising.

Interestingly, the analysis shows that the delivery of illegal IPTV relies substantially on the same 'ecosystem', regardless of the business models employed by the infringers. The ecosystem is defined by the interplay of a number of actors, which correspond to a specific function in the delivery of the illegal service. The analysis has identified 21 actors across four layers of content distribution: content source; hosting network; front-end delivery and applications.

Economic Analysis

Economic analysis is carried out in order to estimate two key elements:

- Number of users accessing unauthorised IPTV content;
- Revenue generated by copyright infringing IPTV subscription providers.

Assessment has been carried out for the whole EU-28 market as well as for each Member State. Main findings suggest that:

**3.6 % Europeans (13.7 million of the EU-28 population)
stream unauthorised IPTV**

**EUR 941.7 million
Unlawful revenue generated by copyright infringing IPTV providers in 2018**

**EUR 5.74
Average single user spends per month on illegal IPTV**

The scale of unauthorised IPTV consumption varies greatly within the Member States. Countries most affected by online illegal IPTV are the Netherlands and Sweden, where almost 9 % of the population is estimated to access unauthorised IPTV. Romania (0.7 %) and Bulgaria (1.3 %) are least affected by illegal IPTV.

When assessing illegal revenue, it becomes apparent that size of market in terms of total population is an important factor. Users in the United Kingdom, France and Germany alone on average spend EUR 532.4 million, accounting for 57 % total revenue made by unauthorised IPTV subscription providers.

Average single user spending on unauthorised IPTV varies significantly among EU countries. Consumers in countries such as Finland, the Netherlands and France are willing to pay more than EUR 6 per month to view unauthorised IPTV. Conversely, people in Slovakia, Hungary and Poland tend to spend only EUR 2.5 per month. It is obvious that consumers vary not only in their willingness to infringe but also in their willingness to pay to access illegal IPTV content. Many factors ought to be considered when defining diverse illegal IPTV price rates, including online piracy rate, perception to infringement, average income and prices charged to access IPTV on legal sources.

Enforcement and case-law analysis

Rights holders can avail of both civil and criminal enforcement measures. Civil enforcement measures apply against both direct infringers and intermediaries, including intermediaries whose services have been used to commit an infringement. In particular, injunctions can be sought against internet access providers to curb IPTV infringements; these include, at least in some Member States, ‘live blocking injunctions’, which block access to streaming servers during the broadcasting of a specific event or series of events. Such injunctions can also be aimed at preventing future infringements, subject to the condition of proportionality. Moreover, internet intermediaries can receive orders to disclose information on infringers; however, disclosure of information on end-users of illegal IPTV services may not be compatible with EU data protection law.

Criminal measures are also available in all EU Member States against IPTV infringers on a commercial scale. Case-law from Member States present significant examples of criminal prosecutions against individuals involved in illegal IPTV. In some cases, long sanctions of imprisonment have been imposed on infringers.

Conclusions and Perspectives

This study contributes to the understanding of the illegal IPTV phenomenon by conducting a comprehensive interdisciplinary analysis of the issue. This report joins legal, economic and technology perspectives in order to carry out an analysis of the illegal IPTV ecosystem. Moreover, this study provides the first quantitative assessment on the magnitude of illegal IPTV in the EU in terms of active users and revenue generated by such illegal activities.

The main findings of this report confirm the notable prevalence of illegal IPTV activities throughout the EU countries. The situation in Member States is not uniform, as many factors such as online infringement rates, perceptions to intellectual property and overall demand for IPTV are distinct. At the EU-28 level, a relevant 3.6 % of the population is engaged in unauthorised IPTV consumption. These users generate nearly EUR 1 billion in unlawful revenue accrued by providers of copyright infringing IPTV. Legislative and technical analysis confirms multiple challenges faced by business and governments when tackling the issue of illegal IPTV.

1. PROTECTION OF TELEVISION BROADCASTS IN THE EUROPEAN UNION

• KEY POINTS

- **Broadcasters' rights cover on-demand streaming but not necessarily live internet streaming.**
- **Only seven Member States explicitly recognise broadcaster's rights in live internet streaming: Austria, Czech Republic, Denmark, Finland, Romania, Sweden and the UK.**
- **Rights holders of works and other subject matter incorporated in TV broadcasts are protected against a wide range of potentially unauthorised acts, including cloud recording, internet retransmission, hyperlinking and indexation of TV broadcasts.**
- **Sporting events as such are not eligible for copyright protection under EU law; however, audiovisual recording of sporting events and works included in such recording (e.g. sound recording, original music and graphic works) are likely to attract copyright under both EU and Member States' laws.**

This section examines the *acquis communautaire* on copyright and related rights with a view of defining the legal boundaries of TV broadcasts' protection in the European Union vis-à-vis unauthorised transmission via internet protocol television (IPTV).

1.1 INTERNATIONAL AND EU LEGAL FRAMEWORK

Broadcasts have been protected internationally for a long time. The Rome Convention, the first legal instrument devoted to the protection of broadcasts for broadcasting organisations, has been in force since 1961. Subsequently, The Convention on the Distribution of Programme Carrying Signals Transmitted by Satellite was signed in Brussels in 1974; its aim was to extend the protection of air broadcasting to satellite broadcasting. Later, the TRIPs Agreement also provided some minimum protection for broadcasting organisations⁽⁶⁾.

The Council of Europe has also attempted to provide some protection with the European Agreement on the Protection of Television Broadcasts (EAT) of June 1960 and with the European Convention Relating to Questions on Copyright Law and Neighbouring Rights in the Framework of Transfrontier Broadcasting by Satellite (European Satellite Convention) of May 1994. In Europe, a number of directives have been implemented that form the current *acquis communautaire* on the protection of broadcasts in the EU, in particular:

⁽⁶⁾ Agreement on Trade-related Aspects of Intellectual Property Rights 1994 (TRIPs Agreement), Article 14(3).

- the Directive on Rental and Lending Rights and Rights Related to Copyright of 1992, consolidated in 2006⁽⁷⁾, establishes for Member States a minimum set of rights in broadcasts that broadly reflect the provisions of the Rome Convention;
- the Satellite and Cable Directive of 1993⁽⁸⁾ and the Conditional Access Directive of 1988⁽⁹⁾ regulate the application of copyright and related rights to, respectively, satellite and cable broadcasting and pay-per-view television services in the Single market;
- the Information Society Directive of 2001⁽¹⁰⁾ harmonises certain rights in broadcasts in relation to the digital environment and the internet.

The Satellite and Cable Directive has been recently amended by Directive 2019/789 on Online Broadcast Transmission⁽¹¹⁾, which will extend to the internet environment some of the rules that currently apply to satellite broadcasting and cable re-transmission. Additionally, the Enforcement Directive of 2004⁽¹²⁾, in conjunction with the Information Society Directive, provides tools to deploy various types of injunctions not only against direct infringers but also (and more effectively) against internet intermediaries. For the latter, however, the 'safe harbour' provisions of the e-Commerce Directive⁽¹³⁾ have to be taken into account.

Infringement of rights in broadcasts may trigger both civil and criminal penalties, although the latter are not addressed by EU legislation. At international level, the TRIPs Agreement requires to provide for criminal procedures and penalties 'at least in case of wilful trade mark counterfeiting or copyright piracy on a commercial scale'⁽¹⁴⁾. All EU Member States comply with the minimum principles mandated by TRIPs.

⁽⁷⁾ Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (codified version).

⁽⁸⁾ Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission.

⁽⁹⁾ Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access.

⁽¹⁰⁾ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

⁽¹¹⁾ Directive (EU) 2019/789 of the European Parliament and of the Council of 17 April 2019 laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes, and amending Council Directive 93/83/EEC.

⁽¹²⁾ Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

⁽¹³⁾ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Sec. 4, 'Liability of intermediary service providers' (Article 12-15).

⁽¹⁴⁾ TRIPs Agreement, Article 61.

1.2 RIGHTS IN TV BROADCASTS UNDER EU LAW: SUBSISTENCE AND OWNERSHIP

TV broadcasts attract two distinct layers of rights:

- rights in the *content* incorporated in TV programmes, which may include copyright in protected subject matter such as literary, musical, artistic and cinematographic works, as well as related rights in sound recordings and performances;
- the broadcasting organisation's right in *broadcasts*, which applies to the programme-carrying signal as such, whether the signal is transmitted over the air, cable or satellite.

These two layers of rights must be assessed separately, as they differ as to the conditions of subsistence, initial ownership and — more importantly to the present study — scope of application on the internet.

1.2.1 Copyright protection of broadcast content

Copyright-protected subject matter under the *acquis communautaire* include any form of expression in the literary, scientific and artistic domain, including cinematographic works⁽¹⁵⁾, photographs⁽¹⁶⁾, computer programs⁽¹⁷⁾ and original databases⁽¹⁸⁾. In a line of cases starting with *Infopaq 1*⁽¹⁹⁾, the CJEU has clarified that the sole criterion to determine the subsistence of copyright is the presence of elements that express the 'intellectual creation' of the author, i.e. elements that depend on the making of 'free and creative choices'⁽²⁰⁾ in the production of the work. In this vein, the court has ruled that sporting events do not qualify as protectable subject matter within the meaning of the Information Society Directive, even though they may be protected by specific legislation of Member States⁽²¹⁾.

While sporting events *as such* do not attract copyright or related rights protection, the audiovisual recording of sporting events may receive protection insofar as it meets the requirement of originality. This is likely to occur insofar as the director is able to make 'free and creative choices' as to where to position the cameras and/or to instruct the camera operators during the match to focus on specific sides of the pitch or moments of the game⁽²²⁾. Similarly, other works and subject matter that are typically included in the recording and transmission of sporting events, such as opening sequence, background

⁽¹⁵⁾ Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version). Official Journal L 372, 27/12/2006, Article 2(1).

⁽¹⁶⁾ *Ibid.*, Article 6.

⁽¹⁷⁾ Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (codified version). Official Journal L 111, 5/5/2009, Article 1(1): 'Member States shall protect computer programs, by copyright, as literary works [...]'.
⁽¹⁸⁾ Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. Official Journal L 77, 27/3/1996.

⁽¹⁹⁾ Case C-312/10 *Infopaq v DDF* [2009] ('Infopaq 1').
⁽²⁰⁾ Case C-145/10 *Painer v Standard Verlags GmbH* [2012] E.C.D.R. 6, § 89-94.

⁽²¹⁾ Joined Cases C-403/08 and C-429/08 *Football Association Premier League Ltd v QC Leisure* [2012] E.C.D.R. 8, § 98-102.

⁽²²⁾ Margoni, T. 'The protection of sports events in the EU: Property, intellectual property, unfair competition and special forms of protection' *IIC - International Review of Intellectual Property and Competition Law*, 47(4), pp. 386-417, 2016, at 398.

sound recording, original music and graphic works, may be copyright protected on their own merits⁽²³⁾. Although in principle *any* original expression can attract copyright under EU law, the court also found that the protectable subject matter must be a ‘work’, namely it must be ‘expressed in a manner which makes it identifiable with sufficient precision and objectivity, even though [...] not necessarily in permanent form’⁽²⁴⁾. It is still an open question whether intellectual creations like TV formats meet this threshold and are protectable on their own.

1.2.2 *The related right in broadcasts of broadcasting organisations*

Unlike copyright in works, the related right in broadcasts is not subject to the originality requirement under EU law and the conditions of subsistence is left to Member States. The right vests in the broadcasting organisation on transmission of the broadcast over the air, cable or satellite.

The broadcasting organisation holds the right in the programme-carrying signal and is typically the licensee of the rights in the content incorporated in the programme. Such licences can be limited both territorially and as to the technical means of transmission, so that for instance a broadcasting organisation may be the exclusive licensee for cable transmission only in a given country. While the organisation can enforce its broadcast rights *erga omnes* in any available jurisdiction, the enforcement of rights in the content incorporated in the programme is limited by the scope of the licence. This point must be taken into due account when examining the available enforcement actions against unauthorised IPTV, as the broadcasters’ rights on the internet are narrower in scope than the rights conferred on authors of original works.

1.3 THE SCOPE OF BROADCASTERS’ RIGHTS ON THE INTERNET

The Rental and Lending Directive gives broadcasting organisations the exclusive right to authorise or prohibit the fixation of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by satellite⁽²⁵⁾. The same directive also confers a narrow ‘public communication’ right, which covers rebroadcasting by wireless means and communication in public places accessible against payment of a fee⁽²⁶⁾. In addition, under the Information Society Directive, broadcasters have the right to reproduce and distribute fixations of their broadcasts, as well as the right to authorise the making available of broadcasts ‘by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them’⁽²⁷⁾. The latter ‘making available right’ applies to all broadcasts, whether the initial transmission is by wire or over the air, including by cable or satellite.

⁽²³⁾ Ibid., § 159.

⁽²⁴⁾ Case C-310/17 *Levola Hengelo BV v Smilde Foods BV* [2019] E.C.D.R. 2, § 40.

⁽²⁵⁾ Directive 2006/115/EC, Article 7(2).

⁽²⁶⁾ Ibid., Article 8(3).

⁽²⁷⁾ Directive 2001/29/EC, Article 3(2)(d).

1.3.1 Making available right: on-demand versus live streaming

Under the Information Society Directive, broadcasts attract rights which are narrower in scope than those pertaining to ‘works’. In particular, broadcasts do not attract the general right of communication to the public⁽²⁸⁾ but only the (narrower) right of making available to the public of fixations of the broadcasts⁽²⁹⁾.

While commentators and national courts have occasionally argued that the making available right may apply to both live and on-demand transmission on the internet, the CJEU clarified in *C More Entertainment* that ‘making available’ refers exclusively to ‘interactive on-demand transmission’ and does not extend to live streaming⁽³⁰⁾.

In the same ruling, however, the court held that EU law does not prevent Member States from extending the scope of the broadcasters’ related rights beyond the acts envisaged in Article 8(3) of the Rental and lending Directive (namely: communications in public places upon payment of a fee), on the sole condition that these rights do not undermine the protection of copyright⁽³¹⁾. This means that the broadcast signal may be protected at national level against a broader spectrum of activities, including most notably simultaneous retransmission via live internet streaming, providing that this extended protection leaves unaffected the ability of rights holders of the content incorporated in the broadcast to exploit the copyright in their works independently.

The protection of broadcasts at Member State’s level will be discussed in section 1.6.2. The table below summarises the scope of protection available under EU law to broadcasters vis-à-vis internet streaming:

Table 1. SCOPE OF BROADCASTING LEGAL PROTECTION AT EU LEVEL

	On-demand streaming	Live streaming
Content included in broadcast programmes	Yes	Yes
Broadcasts’ transmission	Yes	No (but possible at Member State’s level)

1.3.2 Online remote recording of TV programmes

In *VCAST v RTI* the CJEU ruled that the provision of an online service for remote recording of TV programmes constitutes ‘communication to the public’ under Article 3 of the Information Society Directive and is not exempted by the exception for private copying⁽³²⁾. Although the referral related to copyright in the broadcast content and did not raise explicitly a question on the broadcaster’s related

⁽²⁸⁾ Ibid., Article 3(1).

⁽²⁹⁾ Ibid., Article 3(2)(d).

⁽³⁰⁾ Case C-279/13 *C More Entertainment AB v Linus Sandberg*, [2015] E.C.D.R. 15, § 26-27.

⁽³¹⁾ Ibid., § 35.

⁽³²⁾ Directive 2001/29/EC, Article 5(2)(b).

right, the decision of the court applies to both layers of rights, insofar as online video recording constitute an act of making available of fixations of broadcasts⁽³³⁾.

1.4 THE PROTECTION OF BROADCAST CONTENT

In this section, the scope of protection afforded by EU law to copyright-protected works included in broadcast programmes will be considered, with respect to a range of activities that take place in the IPTV environment.

1.4.1 *Reproduction right and the exception for temporary acts of reproduction*

Linear transmission of TV content involves the reproduction of fragments of broadcast at various stages of the technical process. These fragments are temporarily stored in the decoder or in the RAM memory of the computer, depending on the technical means used to transmit the signal, and are created in the end user's TV screen while watching the broadcast.

The question of whether those fragments constitute an actionable act of reproduction under copyright law has been initially addressed by the CJEU in *FAPL v QC Leisure*⁽³⁴⁾, a case on access to satellite broadcast from TV decoders imported from another Member State. To the court, the reproduction right does apply to ephemeral fragments of a work, providing that they contain 'elements which are the expression of the authors' own intellectual creation'⁽³⁵⁾. While sporting events as such do not constitute protectable elements, other works included in the framework of the television broadcast are indeed protectable⁽³⁶⁾. However, the court also ruled that the 'mere reception' of broadcasts and their display in private circles 'does not reveal an act restricted by European Union legislation'⁽³⁷⁾. For this reason, the reproduction of those (fragments of) copyright works can benefit from the exception established in Article 5(1) of the Information Society Directive. Under this exception, temporary acts of reproduction that are merely technical in nature and have the sole purpose of enabling a 'lawful use' of the work do not constitute an infringement of the reproduction right⁽³⁸⁾.

Insofar as the end user does not engage in other restricted acts, such as communication to the public, the CJEU excludes copyright infringement by 'mere reception' of broadcasts by virtue of an act that is not restricted by the applicable legislation — such as importing lawful TV decoders from another Member States without the authorisation of the rights holder. However, a different conclusion applies when the reception of broadcasts is made possible by acts restricted by copyright. In *Filmspeler*, a case on sale of multimedia player with add-ons linking to unauthorised streaming websites, the CJEU ruled

⁽³³⁾ Case C-265/16 *VCAST Ltd v RTI SpA*, [2018] E.C.D.R. 5.

⁽³⁴⁾ Joined Cases C-403/08 and C-429/08 *Football Association Premier League Ltd v QC Leisure* [2012] E.C.D.R. 8.

⁽³⁵⁾ *Ibid.*, § 159.

⁽³⁶⁾ *Ibid.*, § 159.

⁽³⁷⁾ *Ibid.*, § 171.

⁽³⁸⁾ Directive 2001/29/EC, Article 5(1). Please note that the Opinion of the Advocate General in this case had reached exactly the opposite conclusion (Opinion of Advocate General Kokott, Cases C-403/08, § 93).

that the transient copies made in the end user's computer while watching the streaming constitute, as a rule, an infringement of the reproduction right and does not benefit from the exception for temporary acts of reproduction⁽³⁹⁾. This is because the streaming of works protected by copyright from an illegal source is not a 'lawful use' within the meaning of Article 5(1).

While EU law provides for a broad reproduction right, which includes the making of ephemeral fragments of broadcasts streamed from illegal sources, this right is practically of little assistance in the protection of broadcast content over the internet. This function is better served by the right of communication to the public.

1.4.2 *Communication to the public by retransmission of TV signal via the internet*

In *TVCatchup 1*, the Court of Justice held that 'each transmission or retransmission of a work which uses a specific technical means must, as a rule, be individually authorised by the author of the work in question'⁽⁴⁰⁾. The decision establishes that simultaneous retransmission of terrestrial or satellite broadcast signals over the internet is an infringement of the right of communication to the public, even where the broadcast signal is free-to-air and the retransmission covers the same area of reception as the initial transmission⁽⁴¹⁾. Infringement occurs when the retransmission either reaches a new public or employs a different technical means than the initial transmission. This is the case when a broadcast originally transmitted on air, satellite or cable is retransmitted over the internet⁽⁴²⁾. However, simultaneous retransmission to the same public by the same technical means does not constitute communication to the public and does not require fresh authorisation by the rights holders.

The decision leaves unanswered the question of whether a broadcaster that transmits the signal *simultaneously* on air (or on cable) and on the internet is protected against unauthorised live streaming retransmission on the internet. The answer is clearly in the affirmative if the access to the original internet broadcast is restricted by paywall or other technical means (e.g. geo-blocking). This is because the streaming retransmission would either reach a new public (if the signal is taken from the internet transmission) or employ a different technical means (if the signal is taken from the air or cable or satellite transmission). However, when the access to the initial internet transmission is not restricted, it seems inevitable to conclude that no new communication to the public occurs when the signal is retransmitted by unauthorised third parties, or at least not under the argument developed in *TVCatchup 1*.

1.4.3 *Communication to the public by hyperlinking*

A key role in the illegal IPTV environment is played by 'link aggregators'; these are services that collect, index and make available links to streaming content spread on other sites (e.g. cyberlockers or live-streaming providers). Infringement through hyperlinking has been addressed by the Court of Justice in

⁽³⁹⁾ Case C-527/15 *Stichting Brein v Wullems (t/a Filmspeler)*, [2017] E.C.D.R. 14, § 59-72.

⁽⁴⁰⁾ Case C-607/11 *ITV Broadcasting Ltd v TVCatchup Ltd* [2013] E.C.D.R. 9 (*TVCatchup 1*), § 24.

⁽⁴¹⁾ To the court, the finding is supported by analogy with the provisions contained in the Satellite and Cable Directive, which establish that simultaneous and unaltered retransmission by satellite or cable of an initial transmission of a TV programme containing protected works requires fresh authorisation.

⁽⁴²⁾ *Ibid.*, § 39.

six cases⁽⁴³⁾. In *GS Media*, the CJEU has determined the conditions upon which linking to another site where copyright-protected content is made available amounts to an infringement. These are: 1) the copyright owner did not authorise the making available on the initial website, and 2) the hyperlinker had knowledge of the illicit nature of the making available. Such knowledge can be either ‘actual’ (i.e. the hyperlinker has received notice by the rights holder) or ‘constructive’. In determining constructive knowledge, a relevant factor is the profit-making nature of the hyperlinking. Ultimately, this determination can only be done on a case-by-case basis and is left to courts of the Member States.

In cases of illegal IPTV, infringement depends on establishing that the hyperlinker (for example, the aggregator of links to streaming providers) had knowledge of the infringing content. The requirement is easy to meet in most situations⁽⁴⁴⁾.

1.4.3.1 Framing

A different scenario is presented when the audiovisual content that is made available on a website is not just linked but incorporated as such on another website. This method is known as ‘framing’. In *Bestwater*, the Court of Justice held that framing has the same legal effect of linking, in that it does not constitute communication to the public if the audiovisual content was made available on the initial website to the whole internet public, without restrictions, with the authorisation of the copyright holder. In this case, the defendants framed on their websites a video that the claimant had uploaded on YouTube, and the court found no infringement.

Arguably, the ‘*Bestwater* defence’ applies by analogy in case the framed audiovisual content is streamed live (instead of on-demand), subject to the condition that the content was communicated to the whole internet public without restrictions, such as paywall or geo-blocking. However, the question has not yet been referred to the CJEU and uncertainty remains: in at least one case, a national court has interpreted the act of framing unrestricted IPTV as an infringement of the right of communication to the public⁽⁴⁵⁾.

1.4.3.2 Fully loaded set-top-boxes

A special case of infringing hyperlinking is the provision of ‘fully loaded set-top-boxes’, which was considered by the Court of Justice in *Fimspeler*⁽⁴⁶⁾. Applying the conditions established in *GS Media*, the court found that the sale of set-top-boxes equipped with add-ons — essentially hyperlinks to illegal IPTV services — amounted to infringement of the public communication right.

⁽⁴³⁾ Cases C-466/12 *Svensson v Retriever Sverige AB*; [2014] E.C.D.R. 9; C-348/13 *BestWater v Mebes & Potsch* (unreported); C-279/13 *C More Entertainment v Sandberg*, [2015] E.C.D.R. 15; C-160/15 *GS Media BV v Sanoma Media Netherlands BV* [2016] E.C.D.R. 26; C-527/15 *Stichting Brein v Wullems (t/a Filmspeler)* and C-610/15 *Stichting Brein v Ziggo BV* [2017] E.C.D.R. 19.

⁽⁴⁴⁾ See discussion of Member State’s jurisprudence in section 2.

⁽⁴⁵⁾ *Playmedia v. France Télévision 2* February 2016 Appeal Court of Paris (discussed *infra* section 5.1.2).

⁽⁴⁶⁾ Case C-527/15 *Stichting Brein v Wullems (t/a Filmspeler)*.

This case is of paramount importance for the enforcement of rights in broadcasts against unauthorised IPTV, and in section 5 we will see how this jurisprudence is reflected in European jurisdictions⁽⁴⁷⁾.

1.4.3.3 Provision of links on online sharing platform

In *Stichting Brein v Ziggo* the CJEU ruled that the online sharing platform The Pirate Bay, which by means of indexation made possible for end-users to locate and access protected works within a peer-to-peer network, engaged in an act of communication to the public⁽⁴⁸⁾. Arguably this decision applies, more generally, to online platforms that collect, or enable users to share, links to unauthorised audiovisual content providers. As a general rule, the liability of these platforms, which are referred to as ‘link aggregators’ in our analysis of business models⁽⁴⁹⁾, must be scrutinised against the exemptions provided for by the e-Commerce Directive. These will be discussed in section 4.

1.5 LEGISLATIVE DEVELOPMENTS: THE NEW DIRECTIVE ON ONLINE BROADCAST TRANSMISSION

As part of the Digital Single Market strategy, a directive amending the Satellite and Cable Directive has been introduced in 2019⁽⁵⁰⁾. The directive entered into force on 6 June 2019 and must be implemented in Member States’ legislations by 7 June 2021⁽⁵¹⁾.

The directive updates the existing regime for clearance of rights in content incorporated in TV and radio programmes, with the aim of facilitating cross-border provision and access to online services.

More specifically, the directive addresses two distinct kind of services, namely (a) online services that are ancillary to broadcasts and (b) retransmission services that are offered through internet access services. Moreover, it lays down rules for the transmission through direct injection.

1.5.1 Ancillary online services

For online services that are under the control and responsibility of a broadcasting organisation (‘ancillary online services’)⁽⁵²⁾ the directive introduces a ‘country of origin’ principle, whereby the broadcasting organisation must clear copyrights in the content incorporated in its programmes only in the Member State in which it has its principal establishment. The country of origin principle, which mirrors the provision for satellite transmission in the previous directive⁽⁵³⁾, has three important limitations:

⁽⁴⁷⁾ Sections 5.1.4 and 5.3.

⁽⁴⁸⁾ Case C-610/5 *Stichting Brein v Ziggo BV*.

⁽⁴⁹⁾ See *infra*, section 2.

⁽⁵⁰⁾ Directive (EU) 2019/789 of the European Parliament and of the Council of 17 April 2019 laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes and amending Council Directive 93/83/EEC.

⁽⁵¹⁾ *Ibid.*, Article 12.

⁽⁵²⁾ *Ibid.*, Article 2(1) and Rec. 8.

⁽⁵³⁾ Council Directive 93/83/EEC, Article 1(2)(b).

- first, it applies to simulcasting and catch-up services, but not to video-on-demand services⁽⁵⁴⁾ or to services licensed to third parties⁽⁵⁵⁾;
- second, it applies only to news programmes and own broadcaster's productions; sporting events are explicitly excluded⁽⁵⁶⁾;
- finally it leaves intact the freedom to agree limitations, including territorial limitations, on the exploitation of rights in the content incorporated in TV and radio programmes⁽⁵⁷⁾.

1.5.2 Online retransmission services

For services that provide 'simultaneous, unaltered and unabridged retransmission' of an initial transmission (other than by cable, as defined by the previous directive), and which are not under direct control of the broadcasting organisation, the new directive introduces a system of mandatory collective management of rights similar to the one in place for cable retransmission⁽⁵⁸⁾. The system applies only to the content incorporated in TV and radio programmes, not to rights held by broadcasting organisations in respect to their broadcasts⁽⁵⁹⁾. More importantly, when the retransmission is on the internet, the service must ensure that it is carried out in a 'managed environment', namely an environment where only authorised users can access the broadcast⁽⁶⁰⁾. Failing to provide a managed environment would cause the service to engage in a distinct act of communication to the public for which it would need to seek authorisation from the rights holders.

1.5.3 Direct injection

When a broadcasting organisation transmits its programme-carrying signals to a signal distributor by 'direct injection', without transmitting simultaneously the signal to the public, the directive establishes that a single act of communication to the public occurs. The provision on mandatory collective management of rights for online retransmission services applies *mutatis mutandis* to signal distributors⁽⁶¹⁾.

1.6 THE LEGISLATION OF EU MEMBER STATES

The aim of this section is to present an overview of the legal framework in EU Member States, as resulting from both the implementation of the EU *acquis* and the application of national laws. Information was collected by means of a questionnaire distributed to national correspondents in all Member States. The questionnaire required to provide details on the legal protection of broadcasts,

⁽⁵⁴⁾ Directive (EU) 2019/789, Rec. 8.

⁽⁵⁵⁾ Ibid., Rec. 10.

⁽⁵⁶⁾ Ibid., Article 3(1) and Rec. 10.

⁽⁵⁷⁾ Ibid., Article 3(3) and Rec. 10.

⁽⁵⁸⁾ Ibid., Article 4. See Council Directive 93/83/EEC, Article 9.

⁽⁵⁹⁾ Directive (EU) 2019/789, Article 5.

⁽⁶⁰⁾ Ibid., Article 2(3).

⁽⁶¹⁾ Ibid., Article 8.

the main enforcement mechanisms both under the prospective of availability and effectiveness, and the policy initiatives to tackle unauthorised IPTV streaming in every country, either taken by government bodies or private sector organisations (where available).

1.6.1 *Subsistence and ownership*

All Member States have implemented the Rental and lending directive and provide for protection of broadcasts as ‘neighbouring right’, in line with the Rome Convention. They therefore provide broadcasting organisations with the right of fixation of their broadcasts and distribution of these fixations. They also include the right to authorise the retransmission of their broadcasts by air and cable. Transmission by internet is normally not specifically included in broadcasters’ rights, with the notable exception of Romania, where the copyright law gives broadcasters a right to authorise or prohibit ‘retransmission... including retransmission through the internet’⁽⁶²⁾. In the UK, Ireland, and Cyprus, broadcasts are listed among the subject matter entitled to ‘copyright’ protection. In the UK, broadcasts are defined as ‘works’ and enjoy exclusive rights as a copyright work⁽⁶³⁾.

Roughly half of the Member States provide a definition of broadcast, and another half provide the definition of broadcaster. In many cases one definition is provided by law, but not the other.

A few countries provide a more ‘classical’ definition of a broadcaster, which is characterised by its ‘editorial responsibility’ or control over preparation and transmission of the radio or TV transmission. The broadcast is the object of this transmission. The protected transmission is normally by wire or wireless, by satellite or cable and it is a radio or TV transmission. Few countries (Belgium, Estonia, The Netherlands, and Slovakia) have a broader definition of subjects that are defined as ‘media service providers’, who have responsibility on content transmitted over an electronic communication network.

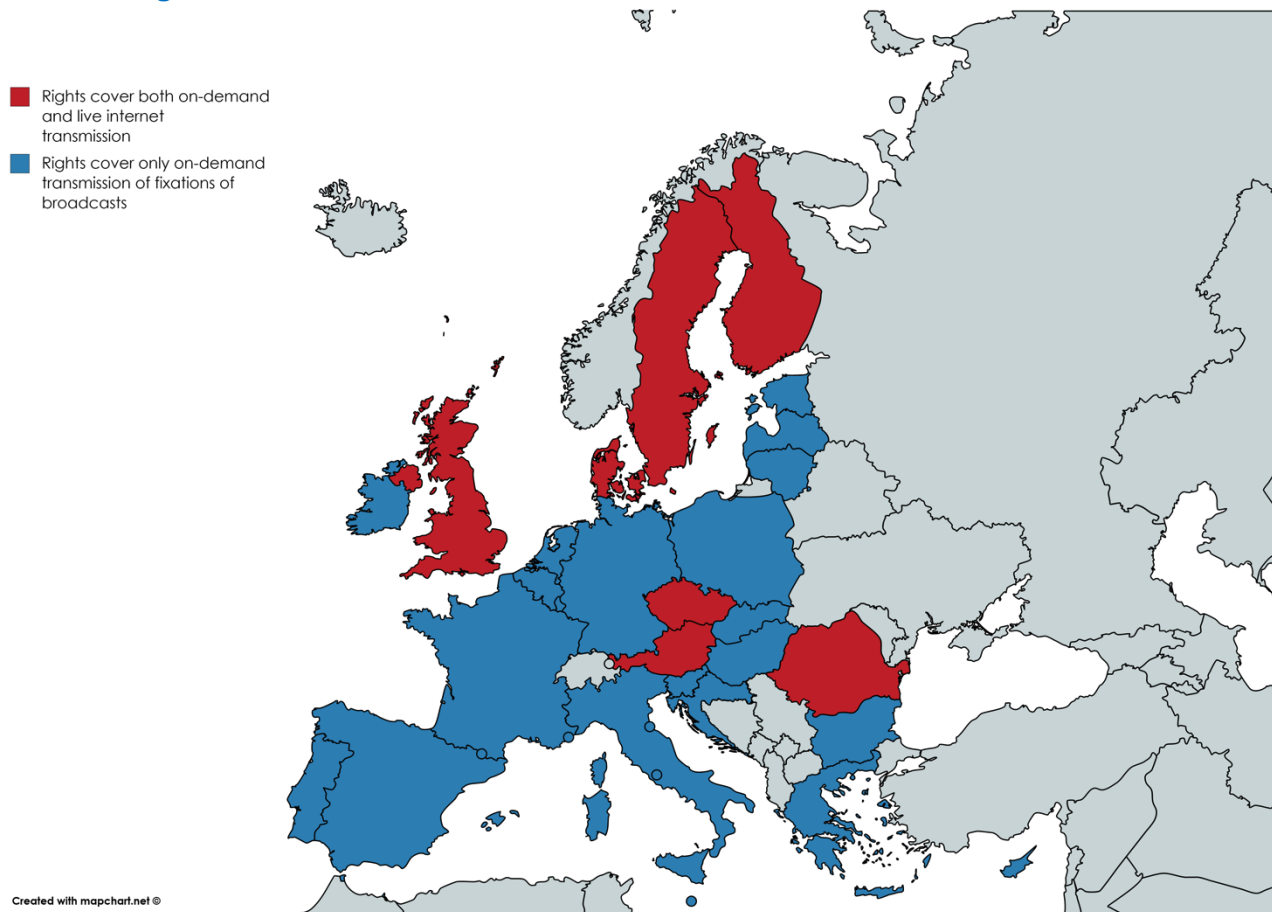
1.6.2 *Scope of the rights: communication to the public*

As discussed in section 1.3.1, the CJEU ruling in *C More Entertainment* (C-279/13) clarified that the making available right provided for by Article 3(2)(d) of the Information Society directive covers only interactive on-demand transmission and cannot be construed as including also live internet transmission of broadcasts. However, in the same ruling the court stated that EU law does not preclude Member States from extending the scope of broadcasters’ rights beyond the provision of Article 3(2)(d), so to include acts falling under the broader right of communication to the public. Domestic legislation provides for extended protection for broadcasts in seven Member States: Austria, Czech Republic, Denmark, Finland, Romania, Sweden and the UK. In all the other countries, broadcasters’ rights are limited to ‘making available’, i.e. on-demand transmission of fixations of broadcasts, and does not cover live internet transmission of those broadcasts.

⁽⁶²⁾ Law No 8/1996 (Romania), Article 129(e).

⁽⁶³⁾ Copyright, Designs and Patents Act 1988 (United Kingdom), Sec. 1(b).

Figure 1. SCOPE OF BROADCASTERS' RIGHTS IN EU MEMBER STATES



In Denmark, Czech Republic and UK, legislation provides explicitly for a general right of 'communication to the public' for broadcasts⁽⁶⁴⁾. In Austria, the wording of the Federal Act providing broadcasters with the 'right to transmit the broadcast simultaneously over another transmitter'⁽⁶⁵⁾ has been interpreted by the Supreme Court as covering also transmission over the internet⁽⁶⁶⁾. In Finland, the Copyright Act provides broadcasters with a right of 'retransmission'⁽⁶⁷⁾. Based on the preparatory material for this provision, in which a technology-neutral approach was stressed, commentators argue that 'retransmission' is broader than 'rebroadcasting' and should include also internet transmission⁽⁶⁸⁾. In Sweden, broadcasters have both a right to make fixations of broadcasts available to the public and

⁽⁶⁴⁾ Copyright Act No 1144 of 23 October 2014 (Denmark), Article 69(1) (broadcasts may not be 'performed in public' without the authorization of the broadcaster, where 'public performance' includes expressly, inter alia, 'communication to the public' (sec. 2(4)(i)); Copyright Act (Czech Republic), Article 84(2) (defining the 'right to use the broadcast' as including specifically '(d) the right to communicate the broadcast to the public'); Copyright, Designs and Patents Act 1988 (UK), sec. 20(1)(c) (communication to the public is an act explicitly restricted in (*inter alia*) 'a broadcast').

⁽⁶⁵⁾ Federal Law on Copyright No 111/1936 (Austria), Article 76a.

⁽⁶⁶⁾ Krone-Hit vs NN, Oberster Gerichtshof 23.02.2016 /4 Ob 249/15v.

⁽⁶⁷⁾ Copyright Act No 404/1961 (Finland), Article 48.

⁽⁶⁸⁾ Harenko, Niiranen, Tarkela: *Tekijänoikeus* 2006, p. 407.

a right to 'exploit' recordings of sounds and images, including by communicating such recordings to the public⁽⁶⁹⁾.

Finally, as referred to in the previous section, Romania gives broadcasting organisations a right to authorise or prohibit 'retransmission... including retransmission through the internet'⁽⁷⁰⁾.

1.6.3 *Limitations and exceptions*

Some Member States provide for specific exceptions for broadcasts, such as the right to record broadcasts for personal use⁽⁷¹⁾, the transmission of broadcasts in a family circle⁽⁷²⁾ or the free public showing of broadcasts⁽⁷³⁾. The specific exceptions for broadcasts provided for by the Information Society directive have been patchily implemented across Member States: while all but three countries⁽⁷⁴⁾ adopt the exception for ephemeral recordings made by broadcasters⁽⁷⁵⁾, in only nine countries⁽⁷⁶⁾ do social institutions benefit from the bespoke exception⁽⁷⁷⁾. However, it is unclear (as it is not specified by the legislation reported) whether these exceptions apply to IPTV broadcasts. In the Netherlands and in Spain, academic literature has argued for the extension of broadcasting exceptions to webcasting (transmission of broadcasts over the internet) but no legislation or case-law confirms this point. In Romania, the legislation specifically states that broadcasting rights include internet retransmission of broadcasts; hence, broadcasting exceptions as well must apply to internet streaming. The UK is a special case, since broadcasts are protected as copyright works and therefore all copyright exceptions apply, including the provisions on fair dealing⁽⁷⁸⁾.

1.6.4 *Legislative developments in Member States*

Little ongoing legislative activity has been reported in Member States in relation to rights in broadcasts. However, some communication authorities have issued recommendations. For example, the Dutch Copyright Commission (The Commissie Auteursrecht) suggested in 2017 to extend broadcasting rights to the online environment.

⁽⁶⁹⁾ Act on Copyright in Literary and Artistic Works, 1960:729, as amended (Sweden), Articles 48 and 46 (read in conjunction with Article 2).

⁽⁷⁰⁾ Law No 8/1996 (Romania), Article 129(e).

⁽⁷¹⁾ Cyprus, Hungary, the Netherlands, Romania, Spain, and the UK

⁽⁷²⁾ Greece, Romania, Estonia, and Portugal.

⁽⁷³⁾ Copyright, Designs and Patents Act 1988 (UK), Sec. 72.

⁽⁷⁴⁾ Austria, Czech Republic and Greece.

⁽⁷⁵⁾ Directive 2001/29/EC, Article 5(2)(d): exception or limitation to the reproduction right 'in respect of ephemeral recordings of works made by broadcasting organisations by means of their own facilities and for their own broadcasts; the preservation of these recordings in official archives may, on the grounds of their exceptional documentary character, be permitted'.

⁽⁷⁶⁾ Belgium, Czech Republic, Cyprus, Denmark, Finland, Italy, Portugal, Romania and Sweden.

⁽⁷⁷⁾ Directive 2001/29/EC, Article 5(2)(e) 'reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons, on condition that the rights holders receive fair compensation'.

⁽⁷⁸⁾ Copyright, Designs and Patents Act 1988 (UK), sec. 29-30.

In the UK, further to the CJEU decision in case C-275/15 (*Catchup II*)⁽⁷⁹⁾, the government has repealed section 73 of the Copyright, Designs and Patents Act 1988, which allowed simultaneous retransmission by cable (including via the internet) in the area of the initial broadcast⁽⁸⁰⁾.

Moreover, in France a new law on audiovisual regulation is planned to be discussed in 2019 aiming to give more competences to HADOPI and to implement also in France the use of 'live' injunctions (injunction to block a live streaming only for the duration of a given sporting event)⁽⁸¹⁾.

1.6.5 The protection of sporting events

As seen in section 1.2.1, sporting events are not a subject matter of copyright protection under EU law. However, a distinction must be made between the event as such and the audiovisual recording and transmission of it. Sporting events attract so-called 'house rights', which gives sports event organisers the possibility to control access to the event venue in accordance with national private law. House rights serve as a legal basis for sports event organisers to negotiate the conditions for audiovisual production companies to record the event⁽⁸²⁾. Audiovisual productions are normally licenced for broadcasting by sports organisations in their basic form (recording of the events, with environment sound and shootings from different camera angles), upon which licensees add action commentaries, graphics superposition of scores and other layout features. Therefore, the live broadcast of a sporting event consists of a complex mosaic of rights. In the UK case of *Football Association Premier League v QC Leisure* the claimant Premier League claimed copyright in up to 25 works falling in the categories of films, artistic works, musical works and sound recordings⁽⁸³⁾.

In some countries, it has been suggested that copyright can protect certain sporting events. In Denmark⁽⁸⁴⁾ and Austria⁽⁸⁵⁾, for example, some type of sports with particular aesthetic value (for example, figure ice-skating) are arguably protected as original works. In addition, some countries provide specific rights for event organisers (see for example France, where sporting events broadcasts

⁽⁷⁹⁾ Case C-275/15 *ITV Broadcasting Ltd v TV Catchup Ltd* [2017] E.C.D.R. 10 (*TV Catchup 2*).

⁽⁸⁰⁾ Digital Economy Act 2017, sec. 34(1)(a) (repealing sec. 73 and 73A of the In the Copyright, Designs and Patents Act 1988). See Government Response to a technical consultation on transitional arrangements following the repeal of Section 73 of the Copyright, Designs and Patents Act 1988 (Intellectual Property Office, 2017).

⁽⁸¹⁾ Lausson, J 04-10-2018 - Politique, 'Ce que propose le rapport Bergé sur l'avenir de la Hadopi et le piratage des œuvres sur Internet, at <https://www.numerama.com/politique/425162-ce-que-propose-le-rapport-berge-sur-lavenir-de-la-hadopi-et-le-piratage-des-oeuvres-sur-internet.html> (accessed 14-6-2019).

⁽⁸²⁾ European Audiovisual Observatory (2016) 'Audiovisual sports rights — between exclusivity and right to information', IRIS Plus 2016-2, p. 13.

⁽⁸³⁾ *FA Premier League v QC Leisure* [2008] EWHC 1411 (Ch), § 179 (Kitchin J.).

⁽⁸⁴⁾ Schovsbo, Rosenmeier, Petersen, *Immaterialret*, 5th edition, 2018, p. 98 and p. 105.

⁽⁸⁵⁾ *Kucsko/Handig, Urheberrecht 2bnd edition Manz Verlag 2017*, § 1 [26], Kuscka et al stipulate further that gymnastics, and synchronised swimming and diving board jumping are generally considered to be unprotectable as the sporting competition is primary here. Similar applies to figure skating where the difficulties of the jumps is prevalent. *Kucsko/Handig, Urheberrecht 2bnd edition Manz Verlag 2017*, § 2 [19]. Something else may be said with regards to ice dancing where an artistic character is more dominant, *Kucsko/Handig, Urheberrecht 2bnd edition Manz Verlag 2017*, § 2 [20]. The mere recording of sport events is not deemed to be protected as film works (*Kucsko/Handig, Urheberrecht 2bnd edition Manz Verlag 2017*, § 4 [37]).

are protected under the French Sports code)⁽⁸⁶⁾. In Portugal, the courts established that specific spectacle rights are recognised to event's organisers, which include sporting events⁽⁸⁷⁾. In the UK case referred to above, the High Court of England and Wales held that albeit sporting events per se are not protected by copyright UK law, namely because they are not included in the closed list of copyright subject matter⁽⁸⁸⁾, single frames of a broadcast signal on a television screen may contain 'substantial parts' of the works included in the screen⁽⁸⁹⁾.

Sports organisations can use other legal provisions to protect their rights on sporting events. For example, they can invoke unfair competition, conditional access agreements (based on 'house rights') and misappropriation⁽⁹⁰⁾.

1.6.6 *Indirect or secondary liability for copyright infringement*

Forms of secondary liability for infringement of copyright and related rights have been recognised in almost all countries, except Cyprus⁽⁹¹⁾, Estonia, Hungary and Romania. In Greece, this form of vicarious responsibility is based on Tort law. In Cyprus and Estonia, it has been reported that ISP taking advantage of the infringement are responsible in the same way as the direct infringer. Interestingly though, Cyprus law establishes a limit to the damages that can be claimed by the rights holder from the ISP, as they cannot exceed the actual economic loss suffered by the victim⁽⁹²⁾.

1.6.7 *Other legislation potentially covering IPTV infringement*

The deployment of other legal instruments to protect broadcasting content, other than copyright infringement actions, is available in all Member States. Trade mark law, unfair competition and contract law are instruments available in all civil-law jurisdictions. In the UK, the common law tort of passing off can provide some form of protection to broadcasting content that is not covered by copyright, such as for instance TV formats.

⁽⁸⁶⁾ Loi n°84-610 du 16 juillet 1984 relative a l'organisation et a la promotion des activités physiques et sportives, Article 18-1.; Code du Sport, crée par Ordonnance n° 2006-596 du 23 mai 2006 relative à la partie législative du code du sport.

⁽⁸⁷⁾ Case nr 4986/06.3TVLSB.S1 Supreme Court Plaintiff vs. RAI & RAI Trade (plaintiff anonymised) 21 May 2009.

⁽⁸⁸⁾ Copyright, Design and Patents Act 1988, Part I ss 3-8.

⁽⁸⁹⁾ *Football Association Premier League v. QC Leisure* [2008] EWHC 1411 (Ch).

⁽⁹⁰⁾ Margoni, T. 'The protection of sports events in the EU: Property, intellectual property, unfair competition and special forms of protection' *IIC - International Review of Intellectual Property and Competition Law*, 47(4), pp. 386-417, 2016, at 17.

⁽⁹¹⁾ Synodinou T. and Jougoux P. 'The legal framework governing online service providers in Cyprus' p. 131 in G. Dinwoodie (ed.), *Secondary Liability of Internet Service Providers*, Springer 2017).

⁽⁹²⁾ *Ibid*, p. 131.

2. SUSPECTED COPYRIGHT INFRINGING IPTV ECOSYSTEM

2.1 BUSINESS MODELS

Analysis shows that a wide variety of business models can be applied when providing access to unauthorised IPTV. Copyright infringing IPTV content distribution ranges from well organised large business structures that sell thousands of monthly subscriptions, to individuals who may only provide streaming access to several consumers via social media. In any case, the unifying element is the product, i.e. access to an IPTV service such as live streamed TV channels. What varies among illegal IPTV providers is the platform, on which the access to IPTV is made available, target audience, pricing strategies and other elements such as complementary products (video on demand, set-top box sales) and social media presence.

Business models applied by illegal IPTV providers are defined in compliance with the methodology developed by the EUIPO (2016) 'Research on Online Business Models Infringing Intellectual Property Rights', Phase 1 — Establishing an overview of online business models infringing intellectual property rights. The base matrix structures business models according to the online platform where unauthorised IPTV content is made available and type of IPR infringing activity⁽⁹³⁾.

Operators in the copyright infringing IPTV market act within the framework of three broadly defined business models:

- **A. 'Illegal IPTV Subscription'** model, where customers are given direct access to IPTV service for a monthly subscription fee ('business to consumer' model).
- **B. 'Illegal IPTV for Resellers'** model, where resellers acquire IPTV packages and other facilities to set up an illegal business ('business to business' model).
- **C. 'Illegal IPTV Free Streaming Portal'** model, where links to streaming websites are collected and made available to users ('business to consumer' model).

Illegal IPTV vendors gain revenue through activities that are designed to take advantage of copyright and related rights infringements. Business models they adapt comprise digital content sharing (access to TV channels) online and on mobile devices, dissemination of malware, illicit collection of user personal data, and contribution to infringement promotion in social media.

The business models are defined in more detail in sections 2.1.1 — 2.1.3. Moreover, an in-depth analysis of twelve representative case studies is presented in Appendix II of this Report.

2.1.1 *Illegal IPTV Subscription*

The most common business model offers a 'package' of unauthorised IPTV services through a dedicated website. The main revenue source within this business model is the direct payments

⁽⁹³⁾ See Appendix II of this Report.

collected from users of unauthorised IPTV. These payments are usually collected as monthly subscription fees. This is defined as a business-to-consumer (b2c) model.

Unauthorised vendors make IPTV content available for direct streaming on their websites or through mobile device applications. These providers operate on the open internet and are commonly reached either via direct browsing or through search engines. Additional exposure on social media accounts such as Facebook or Twitter assists outreach to their target audience, increasing the illegal subscriber base in the EU and promoting their unauthorised services.

Unauthorised IPTV websites also have the technical capacity to spread malware. Pirating hardware which enables free streaming copyright-protected content, e.g. ‘Kodi’ set-top boxes, can come packed with malicious malware. The devices can provide criminals with access to router settings can plant malware on shared network devices and are often leveraged to steal user credentials⁽⁹⁴⁾.

Figure 2. TAXONOMIC MATRIX — ILLEGAL IPTV SUBSCRIPTION

Matrix		Online Digital Platform					
		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
IPR Infringing Activity							
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

⁽⁹⁴⁾ EUIPO (2018), ‘Identification and Analysis of Malware on Selected Suspected Copyright-Infringing Websites’.

The features listed above are common to most unauthorised IPTV providers. Furthermore, unauthorised IPTV streaming websites vary on the basis of parameters such as:

- **Product:** bundles of channels, video on demand (VoD) availability, and hardware purchase option.
- **Pricing strategy:** monthly subscription price, pay-per-view, discount options.
- **Language:** most common language of unauthorised IPTV streaming websites is English. Other frequently encountered languages, such as Spanish, French, Swedish or Turkish target specific national audiences.

2.1.2 Illegal IPTV for Resellers

IPTV resellers make TV content available to be launched on the websites of direct IPTV streaming. Their business model is identified as business-to-business (b2b). These service providers can be categorised as unauthorised IPTV service ‘wholesalers’.

The pricing of IPTV channel packages is lower than that offered directly to subscribers. The main revenue source is payments collected from unauthorised IPTV service ‘retailers’ as monthly or yearly subscriptions. In many instances the ‘business-to-business’ model is combined with a ‘business-to-consumer’ model, as subscriptions are sold to both IPTV resellers and consumers.

Figure 3. TAXONOMIC MATRIX — ILLEGAL IPTV FOR RESELLERS

Matrix		Online Digital Platform					
		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
IPR Infringing Activity							
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

2.1.3 *Illegal IPTV Free Streaming Portal*

Numerous links to websites which enable access to unauthorised IPTV streaming are collected and made available. These providers are also called IPTV ‘link aggregators’.

Such services feature relatively lower streaming quality compared to subscription-IPTV streaming websites. In some cases, these websites stream sports content and are made available for live streaming only. However, many operators maintain vast catalogue of internal and external links to live TV channel streams online. They feature easy access and offer multinational language channels.

As most of streaming content is provided free of charge in these types of websites, unauthorised providers generate revenue through indirect sources, spreading malware or collecting ‘pay-per-view’ and ‘pay-per-click’ payments from advertising⁽⁹⁵⁾.

Figure 4. TAXONOMIC MATRIX — ILLEGAL IPTV FREE STREAMING PORTAL

Matrix	Online Digital Platform	A	B	C	D	E	F
		Internet Site Controlled by Infringer	Third Party Marketplace	Social Media or Blog	Gaming or Virtual World	E-mail, Chatroom or Newsgroup	Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

⁽⁹⁵⁾ Digital Citizens Alliance (2019), ‘Fishing in the Piracy Stream: How the Dark Web of Entertainment is Exposing Consumers to Harm’, April 2019.

2.2 THE ACTORS OF THE ILLEGAL IPTV ECOSYSTEM

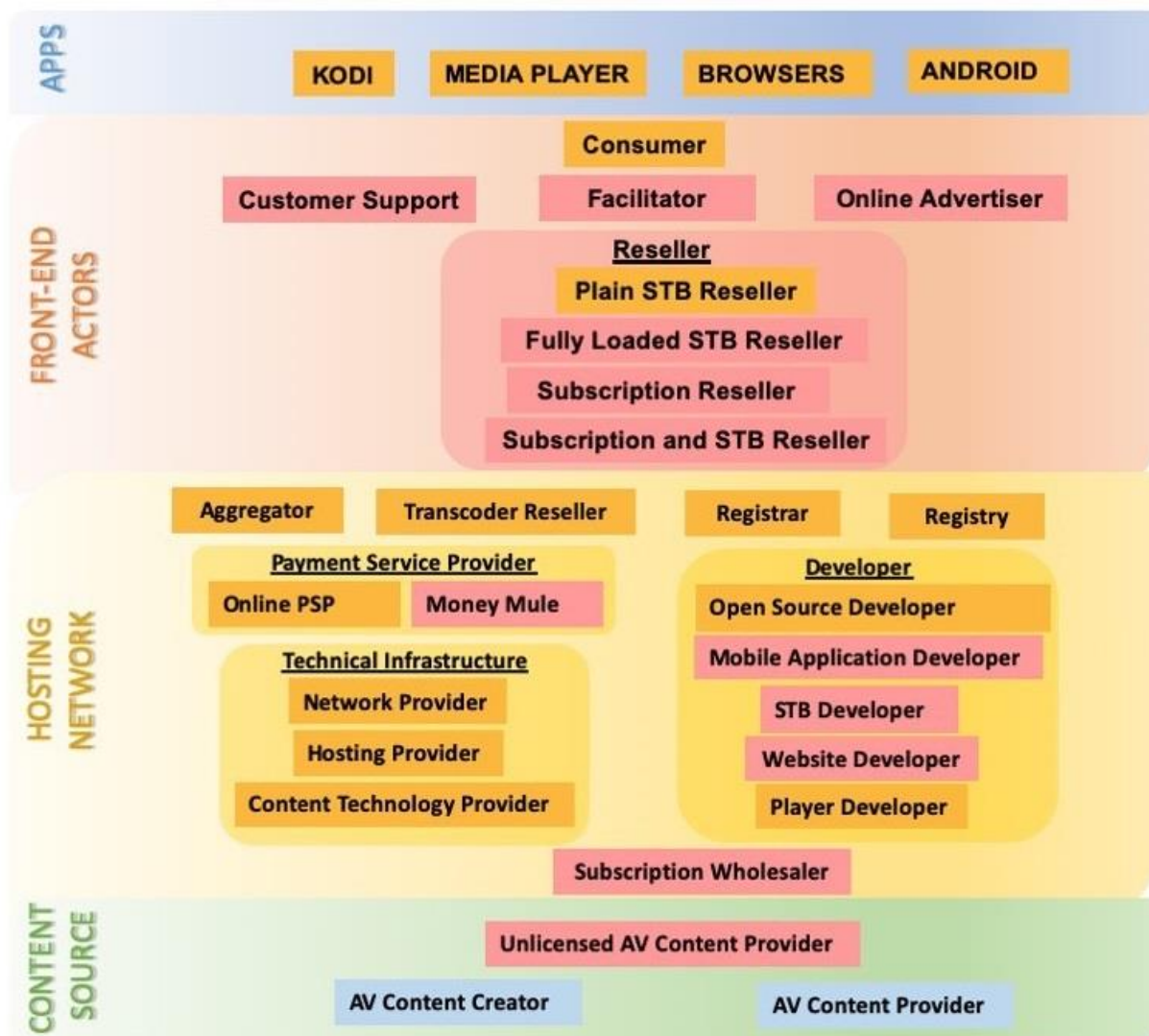
The ecosystem for unauthorised IPTV includes several actors. They consist of primary infringers (the providers of the unauthorised content), a series of active and passive intermediaries, and final consumers. In addition, a number of facilitators and enablers can also be involved by giving instructions and providing tutorials for the installation of middleware — software instrumental for the fruition of the unauthorised content.

Figure 5 provides a high-level overview of the main layers and technical components employed to enable the journey of the infringed audiovisual (AV) stream. These are the essential elements that are common across all business models, which in turn are further enriched through the interaction of the various actors in order to generate cash flows.

Below in the following, overview of the whole ecosystem is provided including the actors, their interaction, their possible legal liabilities and the remedies available against them.

A graphic representation of the IPTV ecosystem and the relations between all actors involved is available in Appendix III.

Figure 5. UNAUTHORISED IPTV DELIVERY



2.3 HOW THE ECOSYSTEM WORKS

The AV piracy ecosystem is comprised of a number of actors, including facilitators and enablers who may be either generic, covering the basic internet and web service provision (such as hosting providers and registrars), or domain specific, in which case they can be of illicit nature. The following sections define the actors referenced throughout this Report.

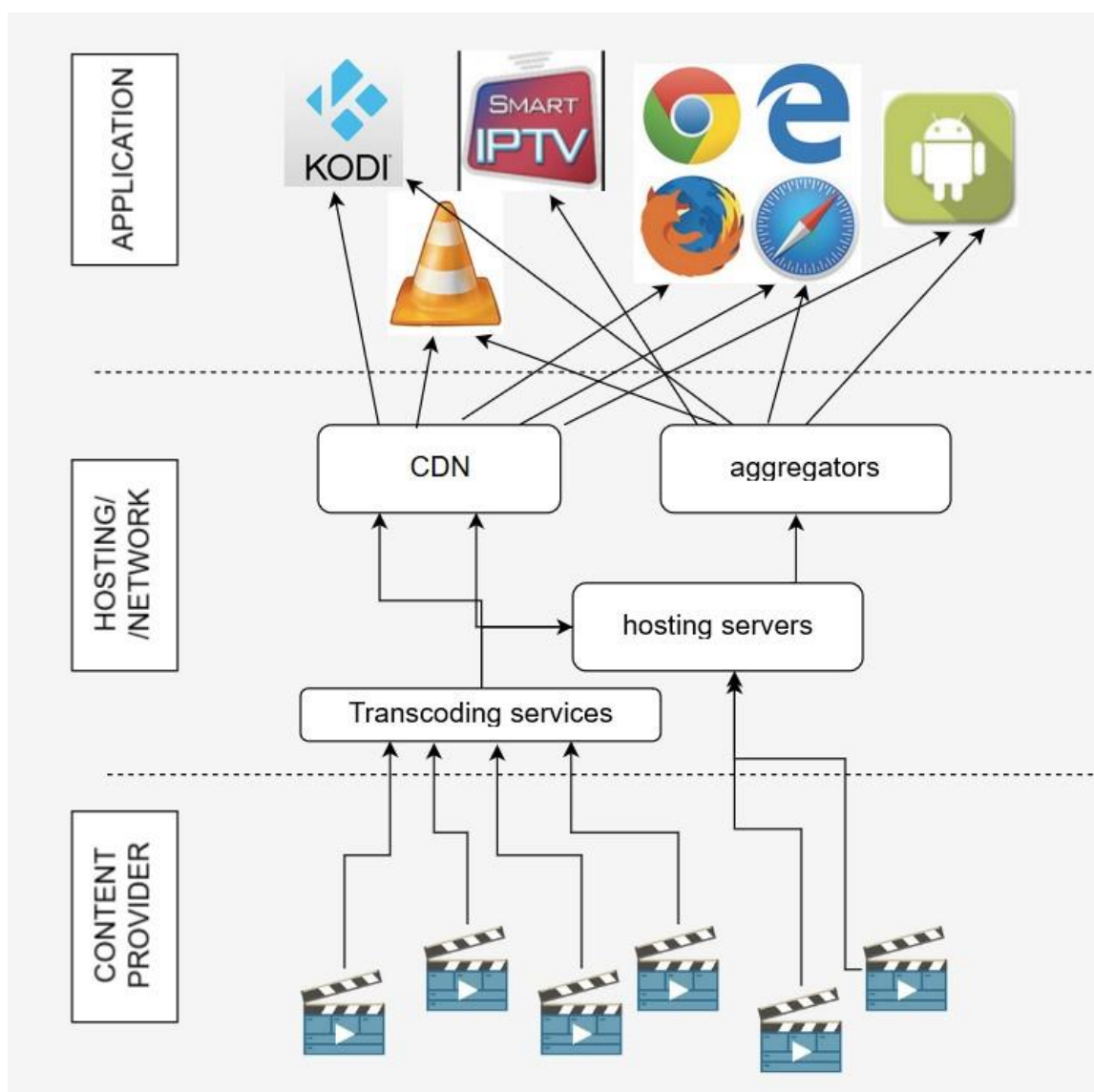
On a very basic level, the infringement commences by an **unlicensed content provider** obtaining legally a stream from a **content distributor** or **content provider** and making it available to third parties, violating thus the terms of use. These third parties may be end users and consumers of the content, or intermediaries, in which case they may also make profit by reselling it.

The content may or may not primarily 'exist' in the internet (cyberspace), in the sense that the content provider may have communicated the content only by other technical means (terrestrial, cable or satellite TV) ⁽⁹⁶⁾. In order to enter the cyberspace, the content will need to pass through **encoding and transcoding services**. These services accept a variety of formats as input and produce a stream that can primarily be delivered by HTTP(s) or RTSP protocols. Transcoding services may be absent if the content is already available on the internet (IPTV type of content). In order for the content to be available to the end users and at a high quality (such as in High Definition), straightforward delivery from a web server is not sufficient. In this case, the content will be delivered through a **Content Delivery Network (CDN)**. In AV streaming, the particular CDNs are specially tuned and configured to achieve an acceptably high throughput and deliver the expected quality of service.

In order for a consumer to be able to discover and access the streams, they are supported by the **aggregators**. An aggregator indexes the streams with the appropriate metadata (title, channel, etc. as well as url) in the form of **m3u** or **m3u8** files. However, as these streams are not necessarily freely available (such as in the case of subscription services), access control is enforced and managed through the **IPTV Panels**. In essence, an IPTV panel manages the subscriptions and channels, acting as a broker between the unlicensed content providers or resellers and the consumers. The **subscription reseller network** is a marketplace for unlicensed AV providers, resellers as well as **wholesale channel sellers**. These actors deploy websites to advertise their business. The subscription (re)sellers depend heavily on the reseller network to create a viable business. In turn, the reseller network may employ **subscription mules** in order to expand the country coverage. These are regular subscribers who agree to share their subscription.

⁽⁹⁶⁾ The nature of the first communication ('traditional' TV broadcasting or IPTV streaming) has some legal effects on the liability of the downstream actors, as discussed in section 1.4.2.

Figure 6. OVERVIEW OF THE KEY COMPONENTS OF TECHNICAL INFRASTRUCTURE FOR DELIVERY OF ILLEGAL IPTV



End users have a wide variety of technological options for viewing the content. These options vary in price and reliability and depend on the customer’s technical capabilities and knowledge, convenience and user experience, as well as hardware equipment. Considering that most likely the end user may have an average quality smartphone, they can directly access content by downloading and installing a streaming app. The most popular apps that can also run on a PC are **Kodi**, **Mobdro**, **Terrarium**, **Popcorn time**, **SPMC**, **Plex** and **Vavoo**. Apps like Kodi do not provide access to infringing sites unless additional functionality (**addons**) is installed. This requires some (minimal) technical knowledge on the side of the end user. Other apps including browser addons provide direct access to infringing sites and can be considered illegal. Apple’s app store and Android’s play store may host streaming apps

for download, irrespective of their infringing nature. However, some apps that have been removed due to their infringing capabilities or are not hosted in the app store in the first place, are available as APKs to be downloaded from third parties. This makes the Android platform a more popular choice for accessing AV content but also increases the risks of infecting the devices with malware.

At the same time there are customised apps that are purpose made. These involve **app developers** modifying existing software frameworks and products to create a branded version of a player. An example of this is **king365tv.com**.

Most of the streaming software can be installed on a PC, either as standalone or as a player addon (e.g. for Kodi). Strictly speaking, the streaming software provides an interface for managing the m3u files that contain the streaming links and EPG information. These files can be opened and the streams can be viewed through any player capable of reading an m3u format, such as VLC. However, to improve the user experience and add intuitive and user-friendly navigation and menus, additional software is used. Many users may also purchase specific hardware to keep permanently connected to their TVs. This is referred to as a **hardware media player** and encompasses a wide variety of devices, such as **Set-top boxes** (STB) and **streaming sticks**. These typically run on one of the three popular operating systems (Android, Linux, iOS). It should be noted that, due to the proliferation of smart TVs, compatible software is now allowed to be directly installed on the TV device itself. A popular app is **Smart IPTV** which is available for Samsung and LG models. In some cases, the underlying operating systems are customised (such as in the case of Enigma boxes) to add strict access controls and anti-piracy evasion mechanisms. The technical savvy end users may elect to buy vanilla devices and configure these themselves, by following instructions found on **forums** and **discussion groups**. Naturally, the variety of models, different configurations options, levels of service but also the anti-piracy efforts and controls, have given rise to **customer support** services. From an illicit business perspective these are overheads directly incurred by the law enforcement Creative Industries efforts to tackle AV piracy through technical and legislative remedies.

Casual and opportunistic viewers who do not invest in specialised devices explore a different range of options; end users who are interested to view a limited number of live events, do this typically through a web browser. They would search for live-streaming aggregators which provide free access to live streaming by linking to unlicensed AV content providers. On this occasion the income for the illegal content provider would come from advertising where the adverts will either appear on the web page or will be superimposed on top of the video (through crafting a **flash object**) prompting and tricking the user to click on fake 'close' buttons and generate pay-per-click income. The aggregator may charge the content provider on a pay-per-link basis, but revenue streams can also be made from other sources, from example by including links to paying websites (typically betting services) as well as via referrals. The more insidious 'free' aggregator sites would allow **malvertising**, where the end-user's system — being a web browser and thus vulnerable to a list of software exploits — will be compromised by allowing the installation of malware. One of the sources the live sporting events aggregators may use is from betting sites which have licenced access but with lower quality streams and 20 second delays.

To complete the ecosystem, there is a relatively large portion of casual video uploaders who do not have a direct financial benefit but enable illegal viewing through uploading on-demand type of content on **cyberlockers**, through P2P exchange platforms, or share credentials of over-the-top services and m3u files for live streams using peer2peer communication apps such as **WhatsApp**, **Signal** and **Telegram**, as well as text storage sites such as **pastebin**. To this end, social media sites are used for both advertising the channel sources for the P2P communication apps, as well as for direct content streaming through misuse of 'live streaming' service such as Facebook Live or YouTube Live.

The actors presented above are the main facilitators and contributors to AV piracy, with the explicit goal to reproduce and deliver or consume AV content with or without a financial gain. To complement this, the core internet backbone services enabling the business models include **Registrars**, **Registries**, **Hosting Providers**, **Search Engines**, **ISPs**, **CDN providers** and **Payment Service Providers**. All these provide the internet infrastructure that the AV piracy business models depend upon. Although these actors are not conducting infringing activities, they need to be considered especially when conducting a forensic investigation. Moreover, some particular service providers (such as CDNs, Hosting Providers, Registries) are preferred by the infringing actors. The main factor for choosing a particular service provider seems to be the geographic/country location i.e. jurisdiction. The preference of a particular service provider can be illustrated by studying the payment providers as an example; most infringing sites prefer cryptocurrency or PayPal payments. It is likely that in a few years cryptocurrencies will become the most popular means of payment, due to the increasing adoption rate of end users. As cryptocurrencies can be potentially anonymous, these may reduce the need and participation of **money mules**, which are present in the current business models. It should be noted that money mules can be both online or offline; the latter are more likely to be conscious of being involved in infringing or illegal activities.

Finally, there are potentially infringing actors (again depending on the respective country's legal framework) who have a direct financial gain, such as **manufacturers** and **(re)sellers of hardware devices (players and transcoders)**, as well as **software developers**, to varying degrees.

2.4 INDIVIDUAL ACTORS

Below is a description of the individual actors involved in IPTV illegal streaming. Every actor corresponds to a specific function in the ecosystem, not to a specific entity. Many entities (private individuals or businesses) can in fact cover several actors.

The representation of the actors is an extension of the STIX⁽⁹⁷⁾ language and format used for exchanging cyber threat intelligence related information.


⁽⁹⁷⁾ <https://oasis-open.github.io/cti-documentation/>

2.4.1 Front-end Actors



Consumer — This is the main actor that supports the market for illegal IPTV business. There are four main subcategories of this actor:

- **Casual viewer (free).** This is a viewer who does not engage in long term relationships with infringers but will occasionally search for freely available AV content. The infringers make profit from this user primarily through advertising and malware infections.
- **Casual viewer (paid).** This is a viewer who will perform a one-off payment to watch specific content (mostly live sports).
- **Long term viewer (STB only).** This is the consumer who may also have technical capabilities to buy and configure a STB. This viewer will make a one-off purchase of the hardware. Less technical consumers will opt to buy a ‘fully loaded’ or pre-configured STB
- **Long term viewer (subscriber).** This is the consumer who may or may not purchase a STB but will perform incurring payments to have ‘premium’ access to AV streaming services.

 By receiving unauthorised IPTV signal on their set-top-boxes, users can commit copyright infringement. Additionally, acquiring IPTV services from illegal providers may in certain cases in principle amount to aiding and abetting. A different issue arises when users share links to streaming services or m3u files with other users, for instance through social media and forums.



(Re)Seller — These can be found on online and in physical marketplaces, and some have dedicated websites. A reseller can fall into one of the following categories:

- **Plain device (re)seller** (aka vanilla device). This refers to the reseller who is not necessarily involved with infringing activities as they are only interested in making profit from hardware sales. There is no need to maintain customer support (other than that relating to sales support, warranty, etc.).
- **Fully loaded device (re)seller.** This is a reseller who provides preconfigured STB/devices, with access to infringing sites. They are only interested in making profit from hardware sales but differentiate their products from those of the plain device reseller in order to be more appealing to a less technical audience. They may offer limited customer support.
- **Subscription reseller.** This refers to a reseller who provides either retransmission or subscription services.



- **Subscription and device reseller.** This is a composite actor comprising of a subscription reseller and a fully loaded device reseller. It is possible for end users to purchase them separately.

While resellers of ‘vanilla’ STB are not liable (unless they provide add-ons or instruction to expand the capability of the device to unlawfully access content), all the other resellers commit direct copyright infringement as well as other criminal offences such as fraud or theft, depending on the jurisdiction. Legal action is easier against hardware resellers, who need to move and store larger volumes of physical goods. Even when subscription resellers are based outside the EU, the deployment of international warrants may be available in some countries.



Facilitator — This is the party who provides tutorials and guidelines on dedicated websites, blogs, social media sites, etc. to show how to configure end user systems to access AV streams illegally. This actor does not necessarily make any profit but can potentially offer paid services to backend actors.

Depending on the level of involvement in the provision of illegal services, the facilitator can be co-liable for IPR infringement and can be prosecuted for aiding and abetting.



Customer support — The parties that have a more formal and defined role than a Facilitator who are mainly found to operate together with subscription resellers.



In many cases customer support is incorporated in the business of the seller or reseller of unauthorised IPTV streaming devices or subscriptions. In this case, at least at a managerial level, it can be found complicit of IPR infringement depending on the case scenario. However, in several instances, customer support is outsourced to third parties. In these cases, it is difficult to presume aiding and abetting, which needs to be specifically proven.



Web search engine — The main source of information and the consumer’s ‘first stop shop’ when looking for infringing services (both free and paid).




Search engines can be required by rights holders to remove URLs from their search results. The owner of the URL that is to be removed normally has the right to respond to the delisting request. In the absence of an expeditious action by the search engine, judicial injunctions can be requested and granted. Leading search engines also have a ‘transparency report’, available to the public, with the indication of the URLs delisted from their services, along with the name of the applicant of the delisting request.



Distribution channel — This refers to the variety of the web-based platforms the device and subscription resellers use to reach out to their customers. Apart from purpose-built sites, the following channels are distinct, each having its own characteristics:



- **Social media platform** — Complementing the search engine, a social media platform is a meeting point for a number of actors where they exchange information, advertise their services and offer support.

 SMPs are considered hosting providers under EU law. They cannot be held responsible for the unlawful behaviour of their subscribers unless, upon receiving notice, they fail to take action. SMPs are misused by a rich variety of infringers, from advertisers (of illegal services), facilitators (helping configuration of illegal devices) to direct content providers (unauthorised). Upon receiving notice of a wrongdoing, they must act expeditiously to remove or disable access to the information.



- **Online marketplace** — Online marketplaces are popular e-commerce platforms used by resellers to promote and distribute their products. Many online marketplaces maintain information on the seller such as reputation scores, contact information as well as statistics on their volume of business.




- **Application store** — The repository of the copyright infringing software. Apart from the two major application stores (Android Play Store and Apple’s App Store), there are also a number of alternatives that allow the download of applications to both smart phones and PCs/laptops.

2.4.2 Back-end Actors




AV Content Producer — This actor refers to the production of the AV content (entertainment, news and sports content), comprising of the organisations and individuals who produce the material and are the initial owners and rights holders.

 This actor typically owns the IPR in the produced content (albeit, for the protection of sport events see section 1.6.5), has standing to sue for copyright infringement and to apply for remedies against infringers and intermediaries, both judicially (injunctions) and extrajudicially (Notice and Take Down, de-listing).




AV Content Provider — The legitimate content provider, located at the very source of the content provision chain. A content provider would create and maintain channels, organise the content sources and liaise with the content producers. The AV Content Provider is typically a broadcasting organisation.

 This actor typically is a licensee of the IPR on the produced content and has standing to apply for remedies against infringement of the rights included in its license. However, if its rights do not specifically include internet transmission, it might lose standing (see section 5.1.1)




Unlicensed AV content provider — This refers to the party who acquires the content legally or illegally and commissions the infrastructure to enable the illegal AV content streaming. This actor has a clear financial gain.

 The direct liability for IPR infringement of this actor is relatively clear. In some cases, the critical mass of the business (large investment and gain) encompasses not only IPR infringement but also organised crime at international level. Remedies are available both in terms of enforcement of rights and seizure of evidence. In practice however, the effectiveness of these measures is subject to the usual difficulties related to bringing proceedings in other jurisdictions.




Wholesale Channel Seller and Resellers — The party selling channel bundles to subscription resellers, part of the subscription reseller network. Their services are not widely advertised, unlike their front actor counterparts (subscription resellers). A wholesale channel seller is closely associated with all types of content providers and especially those controlling outputs from transcoding services.

 These actors very often commit direct copyright infringement as well as contributory infringement. The Seller is likely to be closely linked (if not incorporated) to the Illegal content provider. The same considerations therefore apply regarding its liability and enforcement. The resellers instead are more easily exposed, as they interface with the public, and are the first target of enforcement actions, both from police forces and rights holders. However, the geographical fragmentation of the elements composing their business model makes prosecution and enforcement very difficult and requires strong international coordination.




Subscription Mule — The subscription reseller network depends on subscription mules to expand their coverage of countries. These are regular subscribers who agree to share their subscription. A subscription mule may or may not be aware that they are participating in infringing activities.

 When unaware of the criminal activity that this actor supports, their liability is doubtful. When this person however is aware of the illegal nature of the service it helps to spread, they could arguably be charged with aiding and abetting, depending on the circumstances of the case.




Transcoder (Re)Seller — The party selling transcoding services, primarily in the form of hardware transcoders.

 This actor is not liable as long as his business concerns only the sale of hardware. However, often these products and/or services are integrated in the business models of the **Unlicensed AV content provider**, and therefore their involvement has to be ascertained on a case by case basis.




Aggregator — This is the actor who maintains the information on the location of streaming URLs, by collecting and aggregating hyperlinks to those locations.

 Aggregators commit direct copyright infringement if they have knowledge, or reason to know, that the content made available by the streaming URLs is illegal. There is a presumption of knowledge when they profit, directly or indirectly, from the aggregation of links, or when they intervene by indexing and optimising the links provided by third parties. In this situation, they cannot avail themselves of the exemption for ‘neutral and passive host’ provided for by the e-Commerce Directive and are liable for direct copyright infringement.




Network Provider — This refers to the (legitimate) organisation that provides the infrastructure to deliver the AV content to the end user’s premises. This can involve a variety of technologies (satellite, cable, DSL, etc.), but for this project we refer to the Network Provider as the entity that provides the IP-based network infrastructure.

 This actor is an intermediary providing a service of ‘mere conduit’. As such, it is not responsible for the unlawful content that transits through its services, as long as it does not initiate the communication or modify its content. It is protected from liability under Article 12 of the e-Commerce Directive. However, this does not exclude injunctions. In the context of IPTV enforcement, Network providers are typically the recipient of blocking injunctions directed at disabling access to the infringing content.




Hosting Provider — The organisation that provides the internet working infrastructure (network, web servers, web technologies, racks, etc.) in order to host a web service on behalf of another organisation or individual.

 As long as it provides mere ‘unmanaged’ space, which subscribers rent to build up a web interface to manage access to their customers, this actor is shielded from liability as ‘neutral and passive host’ under Article 14 of the e-Commerce Directive. However, some Hosting Providers may play an active role by facilitating the organisation, optimisation and delivery of the illegal service. Moreover, they may lose the exemption of Article 14 if they receive sufficiently detailed notice of infringements and do not take appropriate action. The liability of this actor can only be assessed on a case-by-case basis, also taking into account the standards and approaches applied by courts in different jurisdictions.




Content Technology Provider — This, together with the Hosting and Network Providers complement the technical infrastructure required for delivering the AV content. The Content Technology Provider covers essentially the components required for delivering an appropriate quality of service, access control and other security mechanisms. A major contribution of the CTP is the implementation and provision of Content Delivery Networks. A representative CTP in this area is Cloudflare.

 This actor and the previous actor are often part of the same business. Their services are not tailored to illegal streaming services as they are general-purpose infrastructures for content delivery. However, some features of specific businesses (typically, anonymity protection, embodied by resistance to injunctions) make them particularly suitable for infringing activity. The CTP liability, therefore has to be ascertained on a case-by-case basis.




Registrar — The organisation who allocates domain names to the public. They are responsible for collecting and keeping updated the contact information on the holders of registered domain names. In order to connect a domain on the internet, the registrar, stipulates the two authoritative name servers (as indicated by the person requesting to register the domain) in the domain registration database of the relevant registry. (These domain servers make sure that when a person requesting access to a domain name, this request will resolve to the correct IP address and thus the person can access to the website).

 According to the Registrar Accreditation Agreement 2013 (lastly updated in January 2019), the ICANN accredited registrar has a duty to verify the contact information of the registrant at the time of registration, and to re-verify periodically such information. The registrar has a duty to take reasonable steps in case the contact information is inaccurate. Specific regulations apply to ccTLDs (e.g. .it, .de, etc.) that are not subject to ICANN. EURid (the registry for the .eu domains) imposes similar obligations on registrars to make sure the data of the domain holder is accurate and up to date; it has the right to revoke the accreditation to the registrars that do not comply with those obligations.



Registry Operator — A registry operator is responsible for allocating the so-called second-level domains. The allocation of second-level domains, which are, in principle allocated by the organisation behind the top-level domain (registry), cannot be applied for directly by any interested party themselves. Instead, operators of a website must engage a domain registrar accredited by the respective registry to perform the registration. The registry maintains the central register in a particular top-level domain (eg. all .es, .de, ... domains), and is responsible for regulating these domains.

 Most ccTLDs are ‘thick registries’, meaning that they collect personal data of the domain holder via the registrar channel. They are exempt from liability as long as they act as ‘mere conduit’.




Payment Service Provider — This actor allows individuals and organisations to accept payments by a variety of different payment methods. This also includes payments using distributed ledger technologies which enable cryptocurrencies.



- **Online PSP** — The legitimate PSPs accepting and processing online payments, such as Paypal, online credit/debit card payments, cryptocurrency platforms, etc.



- **Money Mule** — These parties contribute to payments that can happen in an ‘out of band’ fashion, through physical exchange of money. This makes the investigation more challenging, requiring a wider cyber search scope (i.e. including non-PSP channels, such as email artefacts, call logs, etc.)

 Legitimate payment service providers can be subject to injunctions to provide information or to freeze assets of potential infringers. Moreover, all main payment service providers, including PayPal, adopt policies against illegal transactions and, upon receiving notice from the rights holder, they act against websites that use their services to sell goods and/or services that infringe IPR. However, the use of cryptocurrencies makes the enforcement more difficult in practice. Other Money mules are almost certainly aware of the illegality of their practices, and they can be pursued for aiding and abetting.



Developer — The plethora of different software applications, services and protocols used in AV piracy compose a substantial mosaic of solutions, standards and approaches. Often the developers are the operators of the infringing service or are highly involved in the operation of infringing service (but of course the developers can also be contracted by the operators). Although there is a high level of specialisation and the involved developers have a wide variety of skills, the following classification has been adopted in order to simplify the study:



- **Open Source Developer** — refers to a community of developers who contribute to open source code and publish this on public repositories. Open source projects can have a potentially large support community and the software is freely available to download, use and customize. Due to the economies of scale, a large number of components in the AV piracy ecosystem is open source. This includes software running on the end-user side (such as media players — Kodi, infringing addons, etc.) as well as backend functionality (billing portals, streaming middleware, etc.)



- **Mobile App Developer** — This actor refers to the developer of the mobile (Android and iOS) apps that provide access to infringing sites.



- **Device/media player Developer** — This party is normally a contractor who builds the software image of a particular media player model or family of models. In many cases, this development includes lockdown functionality to enforce ‘vendor lock-in’.



- **Website Developer** — This is the developer for the dedicated infringing web sites (both aggregators and illegal content providers).



- **Player Developer** — This developer is more of an integrator that customises flash type of embedded players to suit the business logic of a particular streaming site.



Like facilitators, software developers can have many roles within the IPTV ecosystem. They can work with or without financial gain and their identity may or may not be hidden behind aliases. Their liability depends on the type of software they develop. It needs to be ascertained, for example, if the software has inbuilt features linking to protected content, or it enables circumvention of paywalls or other technological protection measures. Enforcement depends on traceability as well (contractors or employees are more traceable than anonymous open source developers).



Online Advertiser — this refers to the entity that enables the delivery of the marketing content, mainly by superimposing advertisements on streamed AV content with the aim to generate revenue by coercing the viewer to use the pay-per-click (PPC) advertising business model. As an alternative stream of revenue, the online advertiser may also adopt the cost per impression approach by projecting advertisement content on the aggregator site's advertisement placeholders or inject the advertisements on (free) mobile apps promising or delivering actual AV content.



Advertisers who trade through advertisement networks auctioning impressions have no control and are not aware on which websites their advertisements will be displayed, unless they expressly ask to blacklist certain websites. Most advertisement networks use an automated system to identify illegal websites and avoid placing advertisements on them: to this end, they can receive notice of infringing websites from rights holders and courts. However, illegal websites are frequently designed in a way to mislead the advertisement network.

3. QUANTITATIVE ANALYSIS OF SUSPECTED ILLEGAL IPTV IN THE EU

This section provides an estimate of the magnitude of illegal IPTV in the European Union. The assessment is carried out for the whole European Union (EU-28) single market, as well as at the level of each individual Member State.

In the present report, the purpose of the quantitative analysis is to evaluate two key elements:

- How many users stream unauthorised IPTV content?
- How much income is generated by copyright-infringing IPTV subscription providers?

Estimates show that 3.6 % of the EU population⁽⁹⁸⁾ (13.7 million individuals) access unauthorised IPTV online. In turn, providers of copyright infringing IPTV content generated EUR 941.7 million untaxed revenue in 2018.

The resulting estimates of the users and revenue of unauthorised IPTV for all Member States are shown in Table 2 and Table 3 in relative as well as absolute terms.

**3.6 % EU population
stream copyright
infringing IPTV**

**EUR 941.7 million
Illegal IPTV Revenue
(2018)**

Quantitative methodology applied in this study requires coherent and comparable indicators throughout all Member States. When possible, official data from Eurostat has been used. Additionally, the EUIPO IP Perception⁽⁹⁹⁾ study has been used as an official data source for factors related to online piracy.

Unlawful income gathered by unauthorised IPTV subscription providers is estimated based on an original and rich dataset. The dataset was built for the purpose of this study and gathers information on the content of copyright infringing IPTV service, average subscription prices, subscription period, global website traffic, and type of the website. Data was collected for over 400 online sites that offer streaming access to suspected-illegal IPTV. The methodology is explained in detail in section 3.3.

⁽⁹⁸⁾ Population aged 16-74.

⁽⁹⁹⁾ EUIPO: 'European citizens and Intellectual Property. Perception, awareness and behaviour', March 2017.

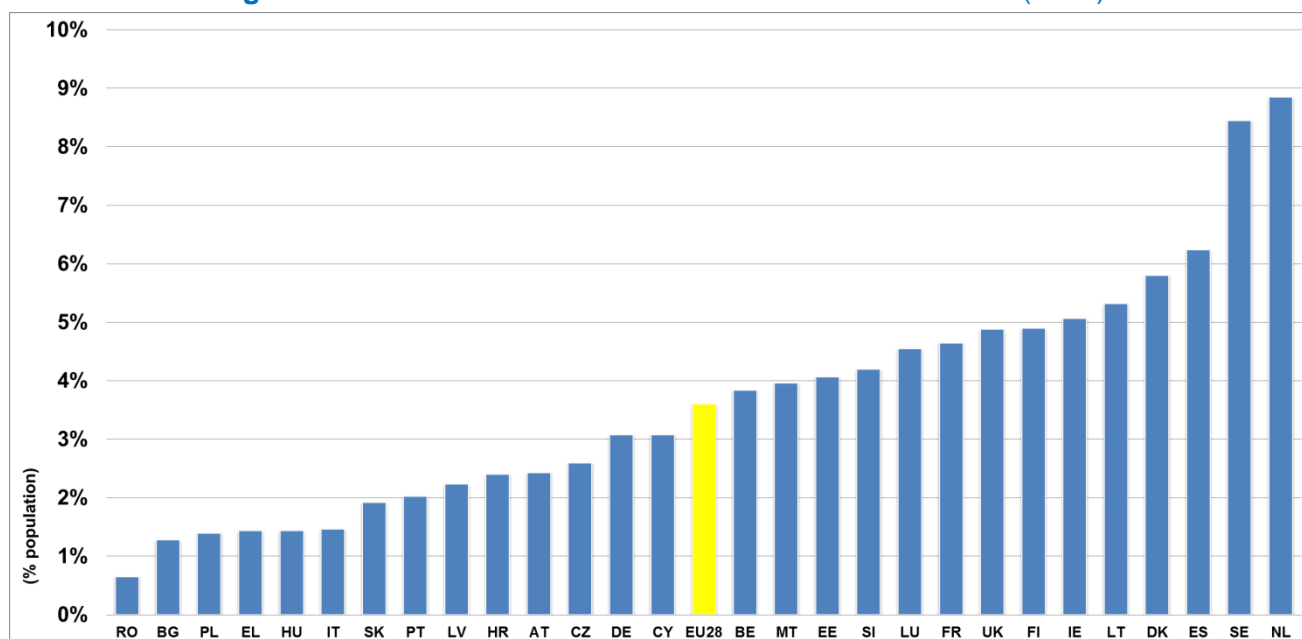
3.1 MAGNITUDE OF ILLEGAL IPTV: USERS

This section provides estimates of the magnitude of illegal IPTV in terms of individuals using unauthorised IPTV service. Estimation is carried out for the whole EU (EU-28) market as well as for each EU country in 2018.

Figure 7 outlines relative shares of total population accessing copyright infringing IPTV. In the European Union, 3.6 % of the population⁽¹⁰⁰⁾ — representing 13.7 million persons — is estimated to watch internet streamed TV (live or catch-up) from unauthorised online sources. This is a considerable share taken into account that the EU market consists of 137 million people who watch internet streamed TV overall⁽¹⁰¹⁾.

The scale of unauthorised IPTV consumption varies between Member States. Countries most affected by online IPTV piracy are the Netherlands and Sweden, where 8.9 % and 8.5 % of the population respectively is estimated to access unauthorised IPTV. Romania and Bulgaria are among the Member States least affected by illegal IPTV — only 0.7 % and 1.3 % of the population is estimated to stream IPTV from illicit online sources.

Figure 7. USERS OF UNAUTHORISED IPTV BY COUNTRY (2018)



Note: Percentage of population aged 16-74.

⁽¹⁰⁰⁾ Population aged 16-74.

⁽¹⁰¹⁾ Based on Eurostat Household Survey 2018.

Table 2. POPULATION STREAMING UNAUTHORISED IPTV IN EU COUNTRIES (2018)

Country	Country code	Share of population accessing unauthorised IPTV	Number of individuals accessing unauthorised IPTV
European Union	EU28	3.6 %	13 680 933
Belgium	BE	3.8 %	320 778
Bulgaria	BG	1.3 %	68 817
Czech Republic	CZ	2.6 %	209 366
Denmark	DK	5.8 %	249 446
Germany	DE	3.1 %	1 909 060
Estonia	EE	4.1 %	39 140
Ireland	IE	5.1 %	170 788
Greece	EL	1.4 %	113 145
Spain	ES	6.2 %	2 158 921
France	FR	4.7 %	2 228 772
Croatia	HR	2.4 %	74 453
Italy	IT	1.5 %	661 924
Cyprus	CY	3.1 %	20 251
Latvia	LV	2.2 %	31 850
Lithuania	LT	5.3 %	111 253
Luxembourg	LU	4.6 %	20 818
Hungary	HU	1.4 %	107 904
Malta	MT	4.0 %	13 543
Netherlands	NL	8.9 %	1 137 343
Austria	AT	2.4 %	162 249
Poland	PL	1.4 %	408 061
Portugal	PT	2.0 %	156 252
Romania	RO	0.7 %	95 806
Slovenia	SI	4.2 %	65 170
Slovakia	SK	1.9 %	81 146
Finland	FI	4.9 %	199 216
Sweden	SE	8.5 %	616 776
United Kingdom	UK	4.9 %	2 361 662

Note: Population aged 16-74 in 2018.

As evidenced in Table 2, countries differ in their relative and absolute shares of users accessing unauthorised IPTV.

In absolute terms, countries with the highest number of persons streaming copyright infringing IPTV are the United Kingdom (2.4 million), France (2.3 million), and Spain (2.2 million). Over 6 million individuals are estimated to have streamed unauthorised IPTV in these three countries in 2018. Together they comprise nearly half (49 %) of the EU's total population engaged in copyright infringing IPTV consumption. Romania, Slovakia, Croatia, Bulgaria, Slovenia, Estonia, Latvia, Luxembourg, Cyprus, and Malta represent a rather negligible share (less than 4 %) of the entire population streaming unlawful IPTV. Less than 100 000 individuals are estimated to access copyright infringing IPTV content in each of these Member States.

Differences between countries are interesting to observe. Many factors come into play influencing people's willingness to access infringing IPTV. As shown by estimates, the quality of internet infrastructure and the penetration of fast broadband can play a bigger role than societies' attitude to IP infringement. Countries like the Netherlands, Denmark, and Sweden tend to have low rates of infringement but high penetration of broadband. Spain represents a case of well-developed internet infrastructure and high level of online infringement. Romania, on the other hand has low rates of both online piracy and internet access.

A recent EU level survey⁽¹⁰²⁾ confirms substantial differences in the level of perception of IP infringement within the European Union. EUIPO report shows that on average 10 % of Europeans 'accessed or downloaded or streamed content from illegal online sources intentionally'. Slovenia is the country with the highest online piracy rate of 20 %, while Romania has the lowest rate of 5 %. Significant differences in online infringement rates suggest that the piracy situation in the single market is not uniform. The reasons for this variation may stem from broadband penetration rates as well as distinct national demand and supply of illicit digital contents.

Proliferation of IPTV viewing habits is another important factor to be taken into consideration. Slovenia and Belgium are countries with high online piracy rates, but few consumers choose to stream TV via internet here. Finland and Germany are countries with similarly developed broadband penetration and rather low rates of online infringement. However, IPTV technology is more proliferated in Finland while users in Germany more often opt for other ways of viewing television, such as cable or satellite.

3.2 MAGNITUDE OF ILLEGAL IPTV: REVENUE

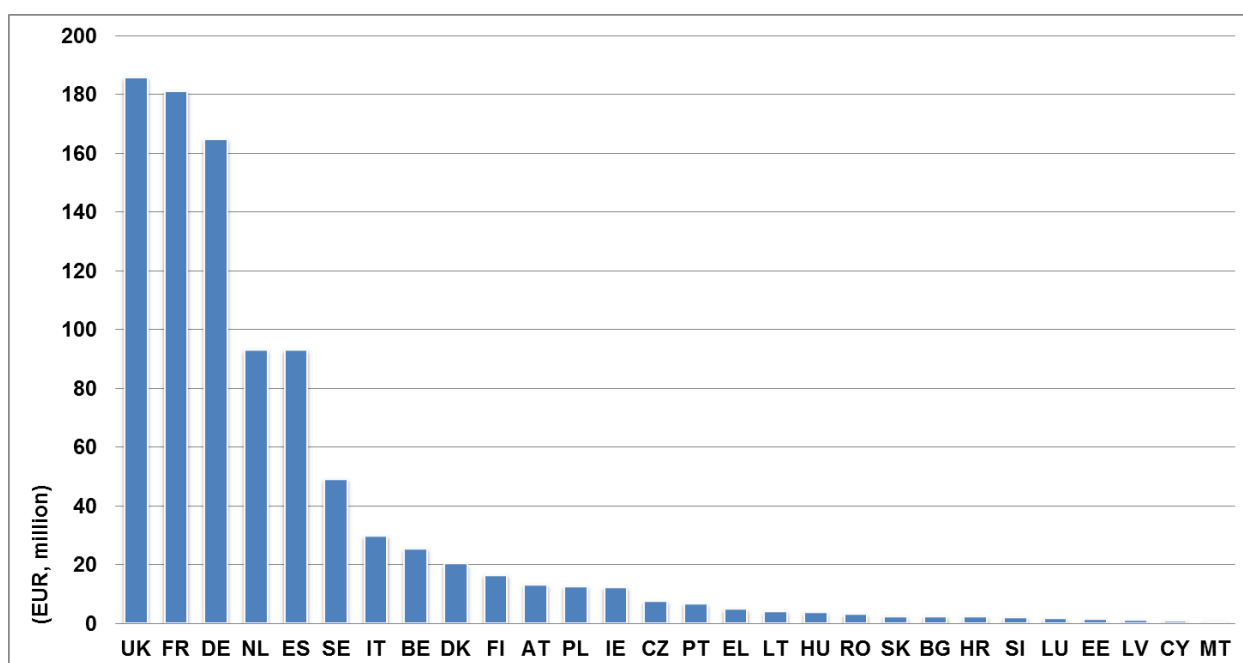
This section provides estimates of the magnitude of illegal IPTV in terms of the revenue that is generated by providers of unauthorised IPTV subscriptions. The assessment is carried out for the whole of the European Union (EU-28) single market as well as at the level of each individual Member State.

⁽¹⁰²⁾ EUIPO: 'European citizens and Intellectual Property. Perception, awareness and behaviour', March 2017.

Results in Table 3 and Figure 8 show both monthly and annual income accrued from sales of illegal IPTV subscription. The unauthorised IPTV subscription market is estimated to generate EUR 941.7 million annual revenue in the European Union in 2018. This amounts to a monthly turnover of nearly EUR 79 million.

Size of the market in terms of users matters, as the largest Member States generate a significant share of unauthorised IPTV revenue. Users in the United Kingdom, France and Germany alone on average spent EUR 532.4 million in 2018. These three countries account for 57 % of the total revenue enjoyed by unauthorised IPTV subscription providers.

Figure 8. ILLEGAL IPTV REVENUE BY COUNTRY (2018)



Note: Revenue generated from unauthorised IPTV subscription sales in the EU Member States in 2018.

Figure 8 outlines the magnitude of illegal IPTV in terms of income accrued from selling unauthorised subscriptions. Estimates show that the top 5 highest spending countries: the United Kingdom (EUR 186 million), France (EUR 181 million), Germany (EUR 165 million), the Netherlands (EUR 93 million), and Spain (EUR 93 million) generate the lion’s share 76 % sales of unauthorised IPTV in the EU single market. Malta (EUR 570 000) and Cyprus (EUR 829 000) are the lowest spending countries.

There are 15 EU countries (Czech Republic, Bulgaria, Estonia, Greece, Croatia, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, Malta, Portugal, Romania, Slovenia, and Slovakia) that each generate less than 1 % of total revenue in the EU’s unauthorised IPTV subscription market. Together these countries account for 4.7 % of unlawful IPTV market income generated in the EU. This might appear a negligible share; however, in absolute terms EUR 44.2 million were generated in 2018, resulting in a monthly income to illegal IPTV providers of EUR 3.7 million.

In relative terms, the largest share (nearly 20 %) of revenue is generated in the UK market. Other significant markets are France (19.3 %), and Germany (17.5 %). Unauthorised IPTV users in these three countries spend close to EUR 532.4 million based on estimates for 2018. In the markets of Spain (10 %) and the Netherlands (10 %) illegal subscriptions to IPTV amount to over EUR 93 million annual spending in each. Romania, where only 0.7 % of the population is estimated to access IPTV illegally — accounts for EUR 3 million annual spending on unauthorised IPTV. This is more than Bulgaria (EUR 2.3 million), but less than Greece (EUR 6.7 million).

Poland and Ireland are countries which both generate similar amount of revenue to unauthorised IPTV providers — EUR 12.5 million. However, Poland's market (408 000 users) is more than twice the size of Ireland's, where only 171 000 users are estimated to stream IPTV from illegal online sources. Users in Poland are willing to spend EUR 2.6 per month on unauthorised IPTV compared to the EUR 6 that users tend to spend in Ireland. These differences are defined by the varied amount of population that is willing to stream paid illegal IPTV instead of accessing free illegal online sources. It is worth emphasising that consumers opting for free of charge infringing access to IPTV are more likely to be exposed to malware and unwanted advertising, and thus face indirect costs.

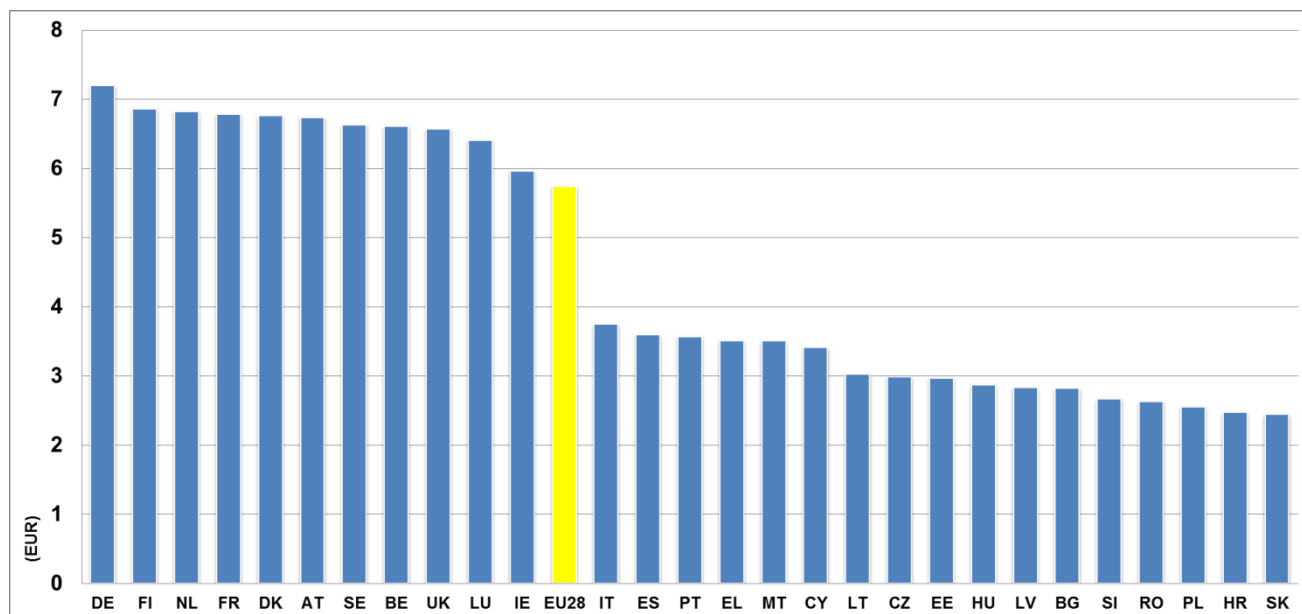
EUR 5.74
Average single user
spending on illegal IPTV
per month

Average monthly and annual spending on unauthorised IPTV is outlined in Table 4 and Figure 9. It represents the amount of revenue that illegal providers of IPTV subscriptions can expect to generate from a single user of unauthorised IPTV services. In other words, it shows how 'profitable' a certain market is to infringing IPTV providers. Differences among countries are significant. Users on average are willing to spend over EUR 6 per month in countries like Germany, France, the Netherlands and Denmark. However, users in Spain, Italy and Lithuania on average tend to spend nearly half — over EUR 3 per month on unauthorised IPTV. Differences among countries can be explained by varied online piracy rates as well as the distinct share of consumers who are choosing to pay to stream infringing IPTV or opt for free of charge yet less convenient free illegal IPTV streaming options.

Table 3. ILLEGAL IPTV REVENUE GENERATED BY UNAUTHORISED IPTV SUBSCRIPTION PROVIDERS BY COUNTRY (2018)

Country	Country code	Monthly Revenue (thousand EUR)	Annual Revenue (thousand EUR)
European Union	EU28	78 470	941 646
Belgium	BE	2 120	25 439
Bulgaria	BG	194	2 329
Czech Republic	CZ	625	7 501
Denmark	DK	1 688	20 252
Germany	DE	13 747	164 967
Estonia	EE	116	1 393
Ireland	IE	1 019	12 228
Greece	EL	397	4 764
Spain	ES	7 756	93 070
France	FR	15 112	181 339
Croatia	HR	184	2 209
Italy	IT	2 481	29 776
Cyprus	CY	69	829
Latvia	LV	90	1 085
Lithuania	LT	337	4 039
Luxembourg	LU	133	1 600
Hungary	HU	310	3 721
Malta	MT	48	570
Netherlands	NL	7 762	93 142
Austria	AT	1 093	13 116
Poland	PL	1 042	12 508
Portugal	PT	558	6 696
Romania	RO	252	3 021
Slovenia	SI	174	2 091
Slovakia	SK	198	2 382
Finland	FI	1 366	16 397
Sweden	SE	4 089	49 072
United Kingdom	UK	15 509	186 109

Figure 9. AVERAGE MONTHLY UNAUTHORISED IPTV COST BY COUNTRY (2018)



Note: average monthly unauthorised IPTV cost for single user in the EU Member States in 2018.

Table 4 and Figure 9 provide estimates of illegal income generated by a single user accessing unauthorised IPTV. In the EU, one user spends an average EUR 5.74 per month on unauthorised IPTV subscription. This amounts to EUR 68.83 annual spending per user.

Variation among Member States is notable. Consumers in Germany on average spend EUR 7.20 per month on copyright infringing IPTV. Consumers in countries like Finland, the Netherlands and France are also willing to pay a relatively high price (more than EUR 6) to view unauthorised IPTV. Conversely, people in Slovakia, Hungary and Poland on average spend EUR 2.5 per month to access infringing IPTV online. In Spain, which has high rates of online piracy and represents a large market, illegal IPTV providers can expect to generate monthly revenue of EUR 3.6 per user.

Estimated average spending rates represent the ‘profitability’ of country markets. The different realities among EU countries are interesting to look at. It is obvious that consumers vary not only in their willingness to infringe but also in their willingness to pay to access illegal IPTV content. Many factors ought to be considered when defining diverse unauthorised IPTV price rates, including online piracy rate, perception to infringement, and average income.

Table 4. AVERAGE MONTHLY UNAUTHORISED IPTV COST PER USER BY COUNTRY (2018)

Country	Country code	Monthly cost per user (EUR)	Annual cost per user (EUR)
European Union	EU28	5.74	68.83
Belgium	BE	6.61	79.30
Bulgaria	BG	2.82	33.85
Czech Republic	CZ	2.99	35.83
Denmark	DK	6.77	81.19
Germany	DE	7.20	86.41
Estonia	EE	2.97	35.60
Ireland	IE	5.97	71.60
Greece	EL	3.51	42.11
Spain	ES	3.59	43.11
France	FR	6.78	81.36
Croatia	HR	2.47	29.66
Italy	IT	3.75	44.98
Cyprus	CY	3.41	40.92
Latvia	LV	2.84	34.06
Lithuania	LT	3.03	36.30
Luxembourg	LU	6.41	76.87
Hungary	HU	2.87	34.49
Malta	MT	3.51	42.11
Netherlands	NL	6.82	81.89
Austria	AT	6.74	80.84
Poland	PL	2.55	30.65
Portugal	PT	3.57	42.85
Romania	RO	2.63	31.53
Slovenia	SI	2.67	32.08
Slovakia	SK	2.45	29.35
Finland	FI	6.86	82.31
Sweden	SE	6.63	79.56
United Kingdom	UK	6.57	78.80

3.3 METHODOLOGY AND DATA

This section describes the methodology of estimating the magnitude of illegal IPTV in the European Union. This report assesses two elements:

- i. Number of users involved in copyright-infringing IPTV consumption in the EU-28 as well as in each Member State.
- ii. Volume of illegal revenue generated by unauthorised IPTV-subscription providers in the EU-28 as well as in each Member State.

3.3.1 Unauthorised IPTV Users

The share of population engaged in unauthorised IPTV service consumption is estimated based on equation number 1 as outlined below:

$$\begin{aligned} & \text{Share of population watching unauthorised IPTV } (N_{U-IPTV,i}) = \\ & \text{Share of population watching Internet streamed TV } (N_{IPTV,i}) \\ & \times \text{Share of population streaming content from illegal online sources } (P_i) \quad (\text{eq. 1}) \end{aligned}$$

The results of the equation 1 estimates are outlined in section 3.1 of this report. Variables considered in equation 1 are the following:

$N_{U-IPTV,i}$ — stands for the share of population engaged in unauthorised IPTV service consumption in a particular EU Member State. This is the result obtained combining two factors described below.

$N_{IPTV,i}$ — stands for the share of population watching internet streamed television⁽¹⁰³⁾ in a particular EU Member State. This population comprises all users that stream IPTV paying for a legitimate subscription, from legal free online sources, or illegal online sources.

P_i — represents share of population that accesses or downloads or streams content from illegal online sources intentionally. In order to estimate the share of users engaged in illegal IPTV streaming, the rate established by EUIPO Report⁽¹⁰⁴⁾ (2017) ‘European Citizens and Intellectual Property: Perception, Awareness, and Behaviour’ is applied. This rate differs in each EU Member State.

⁽¹⁰³⁾ Eurostat indicator ‘Internet use: watching internet streamed TV (live or catch-up) from TV broadcasters, percentage share of persons aged 16-74’. Data is for year 2018. Last update 13/03/2018. Eurostat dataset: isoc_ci_ac_i. Data is based on results of Household Survey 2018.

⁽¹⁰⁴⁾ A recent EU level survey (EUIPO, 2017), shows that on average 10% of Europeans accessed or downloaded or streamed content from illegal online sources intentionally. Data is for year 2016.

Number of persons engaged in unauthorised IPTV service consumption is estimated based on equation number 2 as outlined below:

$$\begin{aligned} & \text{Population watching unauthorised IPTV } (N_{P-IPTV,i}) = \\ & \text{Share of population watching unauthorised IPTV } (N_{U-IPTV,i}) \times \text{Total Population } (TP_i) \quad (\text{eq. 2}) \end{aligned}$$

The results of the equation 2 estimates are outlined in section 3.1 of this report. Variables considered in equation 2 are the following:

$N_{P-IPTV,i}$ — stands for the number of persons (aged 16-74) who are engaged in unauthorised IPTV service consumption in a particular EU Member State. This is the result obtained combining two factors described below.

$N_{U-IPTV,i}$ — stands for the share of population engaged in unauthorised IPTV service consumption in a particular EU Member State. This is the result obtained in equation 1.

TP_i — represents total population⁽¹⁰⁵⁾ (aged 16-74) in a particular EU Member State.

The factors described above allow for assessing the scope of illegal IPTV in each individual EU Member State, as well as in the whole single market. For the purpose of illegal IPTV quantitative estimation, coherent and comparable indicators throughout all Member States are required. This report combines two EU-level surveys when assessing the share of population which streams unauthorised IPTV. First, the Eurostat Household survey (2018) provides the indicator of the overall share of population watching internet streamed television. Second, EUIPO IP Perception study (2017) is applied as a source for the Member State level data on IPTV piracy. More specifically, the IP Perception survey defines the country level rates for unauthorised access to online content. These two indicators, despite arriving from two distinct surveys, provide reliable and comparable EU-28 and Member State metrics.

The only limitation reflected in the IP Perception factors is that this survey does not consider proportions of individuals accessing specific online contents illegally. In the context of this report, IP Perception factor serves as a well-established indicator that allows estimate the levels of online piracy in the EU countries and situate the countries in comparison to the EU-28 average online piracy.

The particular Eurostat Household survey indicator '*Internet use: watching internet streamed TV (live or catch-up) from TV broadcasters*' was chosen after a careful evaluation and an exchange of correspondence with Eurostat experts. The aim was to ensure that this variable comprises users of

⁽¹⁰⁵⁾ Eurostat dataset: Population on 1 January by age, sex and type of projection [proj_15npms]. Data year — 2018. Dataset was last updated 05/02/2019.

both — managed network IPTV as well as internet TV delivered over the top, i.e. open internet. Additionally, Eurostat allows the distinction between the users who are ‘watching video on demand from commercial services’, and users who are ‘watching video content from sharing services’ — these particular services however are outside of the scope of this report.

3.3.2 Unauthorised IPTV Revenue

The monthly revenue that is generated by unauthorised IPTV service providers is estimated based on equation number 3 as outlined below:

$$\begin{aligned}
 & \text{Revenue generated by unauthorized IPTV providers } (R_{IPTV,i}) = \\
 & \text{Population watching unauthorized IPTV } (N_{P-IPTV,i}) \div \text{Average Household size } (H_i) \\
 & \quad \times \text{Share of population paying for unauthorized IPTV monthly subscription } (S_{g,i}) \\
 & \quad \times \text{Average Monthly subscription Price } (P_{g,i}) \quad (\text{eq. 3})
 \end{aligned}$$

The results of the equation 3 estimates are discussed in section 3.2 of this report. Variables considered in equation 3 are the following:

$R_{IPTV,i}$ — stands for the revenue generated by unauthorised IPTV-subscription providers in a particular EU Member State. This is the resulting indicator obtained combining the four factors described below.

$N_{P-IPTV,i}$ — stands for the population engaged in unauthorised IPTV consumption in a particular EU Member State. These figures are computed based on equation 2 in this report.

H_i — stands for the average number of adult equivalents in the household in every Member State. This data is provided by Eurostat⁽¹⁰⁶⁾. One paid subscription per household is considered in order to adjust paid subscription estimation per household instead of an individual person level. This approach results in a more conservative consumer spending estimate. Average household size in the EU-28 is 1.62.

$S_{g,i}$ — represents the share of population that is willing to pay for a monthly unauthorised IPTV subscription. This is the opposite to an option to stream IPTV for free, e.g. from websites that allow direct streaming for certain channels. This share is computed based on a sample of 460 websites that are suspected of providing unauthorised IPTV services. The sample was selected based on careful

⁽¹⁰⁶⁾ Eurostat: Household characteristics by age of the reference person [hbs_car_t314]. Data year — 2015. Dataset was last updated 14/02/2019.

analysis and multiple discussions with cybersecurity experts⁽¹⁰⁷⁾ in the field. It consists of the top visited websites for unauthorised IPTV services in the European Union selected based on a comprehensive search algorithm. The sample allows figuring out the proportions of the internet traffic directed toward different types of unauthorised providers such as subscription IPTV and free-of-charge IPTV streaming.

Thorough analysis of annual website traffic shows that on average nearly 74 % of website traffic is generated by the paid illegal IPTV subscription sites. Distinct shares are applied to four geographical regions that emerge as significantly distinct in their respective proportions of website traffic generated to paid-subscription and to free-of-charge unauthorised IPTV websites. The Member States are grouped into the following regions:

- East-Central EU Member States (Bulgaria, Czech Republic, Estonia, Croatia, Latvia, Lithuania Hungary, Poland, Romania, Slovenia, and Slovakia) are estimated to have 44 % of suspected unauthorised IPTV website traffic that is directed to paid-subscription sites.
- Southern EU Member States (Greece, Spain, Italy, Cyprus, Malta, and Portugal) are estimated to have 52 % unauthorised IPTV website traffic that is directed to paid-subscription sites.
- Western EU Member States (Belgium, Germany, Ireland, France, Luxembourg, the Netherlands, Austria, and the UK) — have the high 92 % share of unauthorised IPTV website traffic directed toward paid-subscription sites.
- Scandinavian EU Member States (Denmark, Finland, and Sweden) — are estimated to generate 86 % of unauthorised IPTV website traffic that is directed toward paid-subscription sites.

P_{g,i} — represents the average unauthorised IPTV monthly subscription price. The prices are deducted based on data collection for 460 suspected-unauthorised IPTV providing websites⁽¹⁰⁸⁾ and varies based on four geographical regions:

- Unauthorised IPTV websites that generate most traffic from East-Central EU Member States (Bulgaria, Czech Republic, Estonia, Croatia, Latvia, Lithuania Hungary, Poland, Romania, Slovenia, and Slovakia) are estimated to charge an average monthly price of EUR 10.36.
- Unauthorised IPTV websites that generate most traffic from Southern EU Member States (Greece, Spain, Italy, Cyprus, Malta, and Portugal) are estimated to charge an average monthly price of EUR 11.55.
- Unauthorised IPTV websites that generate most traffic from Western EU Member States (Belgium, Germany, Ireland, France, Luxembourg, the Netherlands, Austria, and the UK) — are estimated to charge an average monthly price of EUR 11.33.

⁽¹⁰⁷⁾ Experts from Irdeto, Nordic Content Protection and Nagra-Kudelski.

⁽¹⁰⁸⁾ Dataset is created by CIPPM and adapted based on representative sample on suspected unauthorised IPTV providers sourced by Irdeto — one of the leading companies in digital software security and cyberservices.

- Unauthorised IPTV websites that generate most traffic from Scandinavian EU Member States (Denmark, Finland, and Sweden) — are estimated to charge an average monthly price of EUR 11.53.

The weighted average of regional price paid for unauthorised IPTV subscription is estimated based on the equation number 4 as outlined below:

$$Pg_i = \sum_t^i \beta'_t P'_t \quad (eq.4)$$

Equation 4 is a weighted average representing global annual website traffic distribution among distinct types of unauthorised IPTV services. Namely, the unauthorised IPTV is categorised into websites that offer live TV channel streaming, or provide live TV channels streaming in combination with one, two or all three of the following options (t):

- Option to access video on demand, i.e. movies and TV series;
- Option to re-sell unauthorised IPTV subscription;
- Option to purchase hardware, i.e. 'set-top-box'.

The methodology described above allows assessing the scope of income accrued by unauthorised IPTV providers in each individual EU Member State, as well as in the entire single market.

Revenue generated by unauthorised IPTV-subscription providers is estimated based on several data sources. First, the base of users that access unauthorised IPTV is estimated according to equations 1 and 2⁽¹⁰⁹⁾. Eurostat data was used to define average household size in EU countries. Average monthly subscription prices as well as the share of website traffic directed toward unauthorised IPTV subscription websites is estimated based on the original dataset built for the purpose of this report.

In order to carry out quantitative assessment of the income generated by unauthorised IPTV providers in the EU-28 single market as well as in each Member State, detailed analysis of a sample of suspected infringing websites was carried out. An initial dataset based on a list of suspected unauthorised IPTV websites and data on their annual global traffic was provided by the Software Security and Media Technology Company Irdeto⁽¹¹⁰⁾. Thorough check-up and analysis of these

⁽¹⁰⁹⁾ Estimation results are provided in section 3.1 of this report.

⁽¹¹⁰⁾ Irdeto is one of the leading companies in digital platform security, protecting platforms and applications for video entertainment, video games, connected transport and IoT connected industries. With 50 years of expertise in security, Irdeto's software security technology and cyberservices protect devices and applications for some of the world's best-known brands.

websites was carried out in order to confirm their profile. Additional information was collected on the following factors:

- type of unauthorised IPTV service, i.e. — subscription-based, or free-of-charge;
- average monthly subscription prices;
- whether the suspected unauthorised IPTV site offers video-on-demand service alongside streaming of live television channels;
- the possibility to purchase hardware, i.e. a ‘set-top-box’ together with the unauthorised IPTV subscription;
- unauthorised IPTV subscription period;
- option to re-sell the unauthorised IPTV subscription — as some of the websites enable independent IPTV subscription selling.

Finally, the ratio between estimated revenue generated by unauthorised IPTV providers and number of users that are streaming unauthorised IPTV in each Member State is computed. The revenue generated by unauthorised IPTV subscription providers in every EU country is assessed based on equation 5 as outlined below:

$$C_{IPTV,i} = \frac{R_{IPTV,i}}{N_{P-IPTV,i}} \text{ (eq. 5)}$$

The ratio is based on the amount of illegal revenue obtained in a particular EU country ($R_{IPTV,i}$ — defined in equation 3) and number of individuals who are streaming unauthorised IPTV in this country ($N_{P-IPTV,i}$ — defined in equation 2). Resulting estimates are presented in section 3.2 in this report.

4. ENFORCEMENT MEASURES

• KEY POINTS

- **Rights holders can avail of civil enforcement measures against both direct infringers and intermediaries.**
- **A wide spectrum of blocking injunctions can be sought against internet access providers to repress IPTV infringements**
- **Internet intermediaries can receive orders to disclose information on infringers; however, disclosure of information on end-users of illegal IPTV services may not be compatible with EU data protection law**
- **Criminal measures are also available in all EU Member States against IPTV infringers on a commercial scale**
- **Import and sale of IPTV devices may be prohibited on the ground of non-compliance with EU standards on radio equipment**

As discussed in section 2, the ecosystem of suspected copyright-infringing IPTV involves a range of actors, which can be classified according to their proximity to the infringing activity. On the one end of the spectrum there are actors directly and knowingly involved in infringement, and on the other end actors that, albeit playing an essential role in the ecosystem, may not be involved in the infringement. This section examines the measures available to rights holders to enforce their rights against all kind of actors involved in illegal IPTV, starting with intermediaries.

4.1 THE ROLE OF INTERNET INTERMEDIARIES

The delivery of live broadcasting content through the internet requires the involvement of a number of intermediaries. While these actors can attract liability on a number of grounds, the e-Commerce Directive at Articles 12 to 15 creates a set of immunities for a special category of intermediaries, namely ‘information society service providers’ (ISSP)⁽¹¹¹⁾. These broadly conceived immunities exempt, under certain conditions, ISSP from liability for infringements and other wrongdoing committed by recipients of the service. However, they do not preclude the possibility, for a judicial or administrative authority, to impose measures to stop the unlawful behaviour or to demand the disclosure of information on the infringer. In particular, they leave unaffected the ability of rights holders to seek injunctions against ISSP⁽¹¹²⁾.

⁽¹¹¹⁾ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Sec. 4, ‘Liability of intermediary service providers’ (Article 12-15).

⁽¹¹²⁾ See infra, 5.2.

Given the variety of intermediaries involved in the IPTV ecosystem, an assessment of liability is only possible on a case-by-case basis. On a very general level, the *acquis communautaire* allows for a distinction in three broad categories:

- Intermediaries that do not meet the conditions set by the e-Commerce Directive and therefore are not shielded by the immunities. These actors may be held liable for direct copyright infringement.
- Intermediaries whose liability is triggered by actual or constructive knowledge of illegal acts committed by using their services.
- Intermediaries that are under no obligation to act upon receiving knowledge of infringements and can be held liable only upon receiving a court order.

4.1.1 'Active' intermediaries

ISSP benefit from exemptions of liability when their activity 'is of a mere technical, automatic and passive nature', which implies that the ISSP 'has *neither knowledge of nor control over* the information which is transmitted or stored' (113). The CJEU has construed this requirement strictly, as excluding services that provide assistance to the users, for example by 'optimising or promoting' the online sale activities hosted by their services (114).

Although the jurisprudence is not settled, and further guidance is expected from pending referrals (115), the current position clearly excludes from the exemptions those services that systematically and methodically aggregate links to unauthorised IPTV, or that invite users to make those links available on their service. To the extent that they play an active role in the collection, selection and aggregation of links, they are excluded from the beginning from the exemption of Article 14. This means they do not escape liability even if they act expeditiously and remove the link upon receiving notice of infringement. Moreover, as seen in *Stichting Brein v Ziggo* (116), they commit an act of communication to the public and are therefore liable for direct copyright infringement.

4.1.2 Hosting services

ISSP that store information provided by third parties belong to the category of 'hosting' (117). In the IPTV environment, services that provide the internetworking infrastructure (network, web servers, web technologies, racks, etc.) in order to deliver a web service, fall squarely within this category. These services are immune from liability as long as 1) they do not have knowledge of an illegal activity carried out on their services or are not aware of facts or circumstances from which this activity is apparent, or 2) upon obtaining such knowledge, they act expeditiously to remove or disable access to the illegal

(113) Rec. 42 (emphasis added).

(114) Case C-324/09 *L'Oréal SA v eBay International AG* [2011] E.T.M.R. 52, § 123 and Case C-521/17 *Cooperatieve Vereniging SNB-REACT UA v Deepak Mehta* [2018] E.C.D.R. 23, § 50.

(115) In particular the pending referral of the Bundesgerichtshof (Germany) in Case No I ZR 140/15.

(116) *Supra*, section 1.4.3.3.

(117) Article 14

content. Hosting services that do not act after receiving notice of an infringement may become liable to indirect copyright infringement, depending on the laws of Member States⁽¹¹⁸⁾.

The definition of hosting service under the e-Commerce Directive is a very broad and general one and requires a case-by-case assessment. Some ISSP may act as hosting services in some of their functions but not in others. Search engines are a case in point. In *Google v Louis Vuitton*, the CJEU held that a search engine can benefit from the immunity of Article 14 as long as it does not play an active role of such a kind as to give it knowledge of, or control over, the data stored⁽¹¹⁹⁾. According to the AG's opinion in these cases, only partially followed in the Court's judgement, the immunity does not apply to Google's activities related to AdWords⁽¹²⁰⁾. In any event, the main search engines such as Google and Bing respond to rights holders' requests to de-index infringing websites from search results⁽¹²¹⁾.

4.1.3 *Mere conduit and caching*

ISSP that *transmit* but do not *store* information may fall under the category of 'mere conduit'⁽¹²²⁾ or 'caching'⁽¹²³⁾. Network suppliers and internet access providers are examples of 'mere conduit' services. These intermediaries are shielded from liability if they do not play more than a purely technical role in the transmission of the information. As confirmed by the CJEU in *Mc Fadden v Sony Music Entertainment*, access providers that fall under the scope of Article 12 are under no obligation to act upon receiving knowledge of an infringement committed by users of their services⁽¹²⁴⁾. Therefore, rights holders need to obtain a court order to force these ISSP to disable the information.

As far as IPTV is concerned, the most critical question is whether Content Technology Providers (CTS), namely services that provide the technical infrastructure required for delivering the streaming, fall under one of these two categories of ISSP or rather under the (more onerous) 'hosting' exemption⁽¹²⁵⁾. The CJEU jurisprudence does not offer assistance on this point. Although it is difficult to argue that CTS 'store' any information, they nevertheless have the capacity to 'disable' access to live streaming and are the actors that are best placed to do so within the IPTV ecosystem. On this account, they may be held subject to the same obligations as fully-fledged hosting services. However, these services often normally resist rights holders' requests to disable infringing content, and an injunction must be sought to this effect⁽¹²⁶⁾.

⁽¹¹⁸⁾ See supra sec. 2.6.6.

⁽¹¹⁹⁾ Joined Cases C-236/08 to C-238/08, *Google France Sarl v Louis Vuitton Malletier SA* [2010] E.T.M.R. 30, § 120.

⁽¹²⁰⁾ *Ibid.*, Opinion of the Advocate General Poiares Maduro, § 137-146.

⁽¹²¹⁾ See infra, section 4.2.4.

⁽¹²²⁾ Article 12.

⁽¹²³⁾ Article 13.

⁽¹²⁴⁾ Case C-484/14 *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH* § 58-59.

⁽¹²⁵⁾ A similar issue has been addressed by US courts in the context of proceedings against CloudFlare.

⁽¹²⁶⁾ Husovec, M. (2017) *Injunctions Against Intermediaries in the European Union*, Cambridge University Press, p. 219-20.

4.2 CIVIL ENFORCEMENT MEASURES

Irrespective of establishment of liability, EU law ensures that rights holders have the possibility to apply for an injunction against intermediaries whose services are used by third parties to infringe their Intellectual property rights (IPR) ⁽¹²⁷⁾. The term ‘intermediary’ is broader than ISSP and includes every actor who engages in an economic activity in the course of which he or she is in a position to prevent third-party infringements ⁽¹²⁸⁾. Some of the actors that the CJEU found falling within the definition of intermediary for the purpose of receiving an injunction include internet access providers ⁽¹²⁹⁾, social media platforms ⁽¹³⁰⁾, auction websites ⁽¹³¹⁾, an operator of open wireless ⁽¹³²⁾.

The scope of injunctions against internet intermediaries has been discussed by the CJEU in a number of cases. For the purpose of this study, it suffices to recall the following general principles that can be extracted from the CJEU jurisprudence:

- injunctions can be aimed at both repressing an existing infringement and preventing future infringements ⁽¹³³⁾;
- they must be effective, proportionate and not impact on fundamental rights and freedoms of intermediaries ⁽¹³⁴⁾ and internet users ⁽¹³⁵⁾;
- they do not have to lead necessarily to a complete cessation of the infringement ⁽¹³⁶⁾.

With this in mind, the following sections will discuss the key types of injunctions available to deter IPTV infringements.

4.2.1 Blocking injunctions

The most widely used type of injunction in connection with IPR online infringements is the blocking injunction, i.e. an order to internet access providers to block users’ access to a certain list of websites. These injunctions have proven to be more effective than orders or requests to hosting service providers to take down offending websites. This is because operators of these websites can easily move to another hosting service, and to move again to hosts based in remote jurisdictions which do not respond to notice and takedown requests. By contrast, blocking injunctions to internet access

⁽¹²⁷⁾ Directive 2004/48/EC, Article 11 and Directive 2001/29/EC, Article 8(3).

⁽¹²⁸⁾ M. Husovec, *Injunction s Against Intermediaries in the European Union*, p. 90.

⁽¹²⁹⁾ Cases C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH* [2009] ECLI:EU:C:2009:107; C-70/10 *Scarlet Extended v SABAM* [2012] E.C.D.R. 4, and C-314/12 *Telekabel v Constantin Film* [2014] E.C.D.R. 12.

⁽¹³⁰⁾ Case C-360/10 *SABAM v Netlog NV* [2012] 2 C.M.L.R. 18.

⁽¹³¹⁾ Case C-324/09 *L’Oréal SA v eBay International* [2011] E.T.M.R. 52.

⁽¹³²⁾ Case C-484/14 *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH* [2016] E.C.D.R. 26.

⁽¹³³⁾ Case C-324/09 *L’Oréal SA v eBay International*, § 128-134.

⁽¹³⁴⁾ Case C-360/10, *SABAM v Netlog NV* § 46-51.

⁽¹³⁵⁾ Case C-275/06 *Promusicae v Telefonica* [2008] E.C.D.R. 10, § 64 and Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH*, [2014] E.C.D.R. 12, § 55.

⁽¹³⁶⁾ Case C-314/12 *Telekabel v Constantin Film*, § 58-63.

providers make the website unavailable to users in the country where the order is made regardless of the host where the website is located⁽¹³⁷⁾.

The CJEU in *Telekabel* has found this type of injunction compatible with EU law, providing that they do not deprive internet users from the possibility of lawfully accessing the information available, and they have the effect of preventing (or of making more difficult) the access to infringing content⁽¹³⁸⁾.

4.2.2 *Dynamic injunctions*

Blocking injunctions can specify not only the domain name and IP address of the website(s) to block access to, but also any further domain names under which infringements relating to the same rights are committed. Such ‘dynamic’ orders extend the efficacy of blocking access to a website and allow preventing future infringements. Although it may be argued that those orders are in line with the existing CJEU jurisprudence, no referral to the CJEU has yet been made on their compatibility with EU law.

4.2.3 *Live blocking injunctions*

Blocking Injunctions can work by requiring internet access providers to block users’ access to servers hosting infringing streams of live sporting events. The so-called ‘live’ blocking orders are particularly effective in tackling illegal IPTV, as they target specifically the servers that stream illegal content during live events broadcast. These orders have been first issued in the UK⁽¹³⁹⁾ and are rapidly gaining popularity in other EU Member States as well⁽¹⁴⁰⁾.

4.2.4 *De-indexing injunctions*

These injunctions request search engines to de-index infringing websites, so that the links to those websites do not appear in the list of search results. Orders to de-index video streaming websites have been issued in France⁽¹⁴¹⁾ and in Portugal⁽¹⁴²⁾. Major search engines adopt a policy of de-indexing websites that violate their terms and conditions (which include respect of IPR) upon receiving notice from the rights holder.

4.2.5 *Disclosure of information*

A court order can impose to internet access providers the disclosure of the identities associated with IP addresses used to infringe copyright. This remedy has been used extensively in the years 2000-2010 in the USA by the recording industry, in the context of so-called ‘John Doe proceedings’ against

⁽¹³⁷⁾ See the detailed discussion in *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch) (Arnold J.).

⁽¹³⁸⁾ *Ibid.*

⁽¹³⁹⁾ *Football Association Premier League Ltd v British Telecommunications Plc* [2017] EWHC 480 (Ch).

⁽¹⁴⁰⁾ See *infra* section 5.2.1.

⁽¹⁴¹⁾ *Microsoft v Association de Producteurs de Cinéma*, Tribunal de Grande Instance, Paris, 28 Novembre 2013.

⁽¹⁴²⁾ Case No 49/15.9YHLSB, Intellectual Property Court of Lisbon, 30 March 2015.

users who engaged in illegal file sharing of music. Similar strategies have been applied in Europe as well with alternate success, with some national courts refusing to grant an injunction to disclose personal information on the ground of prevailing privacy rights of the individuals⁽¹⁴³⁾.

The legitimacy and scope of disclosure of information has attracted the scrutiny of the CJEU in several cases. In *Promusicae*⁽¹⁴⁴⁾ the court ruled that the Enforcement Directive does not preclude Member States from laying down obligations to disclose personal data in the context of civil law proceedings (although nor does it require it). However, such obligations need to ensure a fair balance between the rights of copyright holders and those of internet users and must abide the principle of proportionality. The point has been reiterated in *LSG v Tele2*⁽¹⁴⁵⁾ and in *Bonnier*⁽¹⁴⁶⁾. In the latter case, the court ruled that the obligation laid down by Sweden was likely to ensure a fair balance between the rights involved. Under Swedish law, for an order for disclosure to be made, the claim must satisfy three conditions, namely a) there must be clear evidence of an infringement, b) the information must facilitate the investigation of the infringement and c) the reasons for the measure must outweigh the nuisance or harm suffered by the person affected.

This remedy has not been used so far in the context of illegal IPTV, and it is questionable whether national courts would allow disclosure of end users' personal information. A different set of considerations applies to disclosure orders targeting other actors of the illegal IPTV ecosystem, such as sellers and resellers of illegal IPTV services and devices. In this connection, the order issued by an English court against IPTV subscribers to identify the persons who had provided them with the goods and/or services to screen infringing football games seems proportionate and in line with CJEU jurisprudence⁽¹⁴⁷⁾.

4.3 CRIMINAL ENFORCEMENT MEASURES

In addition to civil enforcement measures harmonised by the Enforcement Directive and the Information Society Directive, EU Member States also apply criminal procedure and penalties to ensure enforcement of intellectual property rights, in line with Article 61 of the TRIPS Agreement⁽¹⁴⁸⁾. A previous study has shown that in all Member States, 'any person or entity who intentionally (or in some countries grossly negligently) infringes an IPR may not only be subject to a civil lawsuit filed by the rights holder, but may also be subject to criminal sanctions in particular to fines or imprisonment, but also to seizure of the infringing goods and to confiscation of profit'⁽¹⁴⁹⁾. Due to lack of harmonisation, however, these measures vary significantly across Member States. Criminal

⁽¹⁴³⁾ Giovannella, F. *Copyright and Information Privacy*, Elgar, 2017, p. 103; EUIPO (2018), 'IP Enforcement. Case-law collection on the balance between the right of information and fundamental rights in the European Union'.

⁽¹⁴⁴⁾ Case C-275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] E.C.D.R. 10.

⁽¹⁴⁵⁾ Case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH* [2009] ECR I-01227.

⁽¹⁴⁶⁾ Case C-461/10 *Bonnier Audio AB v Perfect Communication Sweden AB* [2012] E.C.D.R. 21.

⁽¹⁴⁷⁾ *Football Association Premier League Ltd v Wells* [2015] EWHC 3910 (Ch).

⁽¹⁴⁸⁾ See *supra*, sec. 2.1.

⁽¹⁴⁹⁾ EUIPO (2018), 'Study on Legislative Measures Related to Online IPR Infringements', p. 30.

proceedings against infringers of intellectual property rights are normally initiated by a complaint of the rights holder, but judicial authorities can sometimes initiate proceedings *ex officio* when an infringement is classified as a public crime. This is normally the case when certain aggravating circumstances occur, such as infringements involving money laundering and/or carried out by organised criminal groups⁽¹⁵⁰⁾. In most cases, criminal prosecution involves procedures that apply both to infringement of intellectual property rights and other kind of illicit behaviour, such as forgery, fraud, conspiracy and inchoate offences like assisting the commission of an offence⁽¹⁵¹⁾.

Criminal sanctions include imprisonment, with maximum possible sentences ranging from two to ten years. In most Member States surveyed, the penalties available are organised in a broad range, starting with the imposition of fines for less severe offences⁽¹⁵²⁾.

4.4 ADMINISTRATIVE PROCEDURES

The Enforcement Directive mandates Member States to provide rights holders with the possibility of applying for injunctions against intermediaries, but leaves to national law to determine the conditions and procedures relating to such injunctions⁽¹⁵³⁾. While in all Member States such injunctions require judicial proceedings, in Italy they can also be granted by AGCOM, the authority of telecommunications, following an expedite administrative procedure⁽¹⁵⁴⁾. The targets of such procedure are 'mere conduit' and 'hosting' services. The procedure allows rights holders to request an internet service provider to remove or block access to websites hosting allegedly copyright infringing material, or a website to take down infringing content and refrain from re-uploading it. AGCOM can impose fines in case of non-compliance with the orders.

A similar procedure has been recently established in Greece. Under this procedure, rights holders can file an application to a dedicated Committee set by the Hellenic Copyright Organisation, which is vested with authority to request internet service providers to remove or block access to infringing content⁽¹⁵⁵⁾.

⁽¹⁵⁰⁾ Ibid.

⁽¹⁵¹⁾ See examples *infra*, sec. 6.3.

⁽¹⁵²⁾ EUIPO (2018), 'Study on Legislative Measures Related to Online IPR Infringements', p. 64.

⁽¹⁵³⁾ Directive 2004/84/EC, Rec. 23.

⁽¹⁵⁴⁾ Delibera 680/13/CONS, 'Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70'.

⁽¹⁵⁵⁾ Law No 4481/2017 on Collective Management of Copyright and Related rights, Multiterritorial Licensing of Rights in Musical Works for Online Use and Other Matters in the Competence of the Ministry of Culture and Sports. See T. Chiou 'Greece: new notice and take down administrative mechanism for online copyright cases now in force', *IPKat* 5 March 2018, <http://ipkitten.blogspot.com/2018/03/greece-new-notice-and-take-down.html>.

4.5 CUSTOMS MEASURES REGARDING STREAMING DEVICES

According to European crime assessment reports, IPTV piracy is expected to grow in the future with the diffusion of applications for computers, phone and tablets which will probably replace IPTV devices⁽¹⁵⁶⁾. Meanwhile, import and trade of set-top boxes (STB) is still under way and represents a key asset for the leading business models in the IPTV piracy ecosystem⁽¹⁵⁷⁾. The IP Enforcement Directive requires Member States to adopt enforcement measures to protect IP rights, including seizure of goods suspected of infringing to prevent their entry into the market⁽¹⁵⁸⁾. In addition, the Regulation on customs enforcement of intellectual property rights⁽¹⁵⁹⁾ allows certain customs activities including seizure and detainment of goods suspected to be infringing IP rights such as patents, utility models, trade marks, registered geographical indications, registered designs and models, copyright and related rights.

Enforcement in the field of illegal IPTV, however, presents specific challenges. This is because while fully loaded STB are infringing copyright⁽¹⁶⁰⁾, and they fall squarely within the scope of the Enforcement Directive and the IP Customs Regulation, ‘vanilla’ devices (i.e. STB that are not yet configured to receive illegal streaming) do not directly infringe any intellectual property right. These devices can be sold as such to end users, who will then configure them themselves by following instructions provided by the reseller or found on forums and discussion groups⁽¹⁶¹⁾. However, ‘vanilla’ devices manufactured by dubious businesses may present hazardous features that make them illegal under EU safety standards. This may in turn represent an alternative path for enforcement⁽¹⁶²⁾.

The Radio Equipment Directive of 2014 (RED) in fact establishes a legal framework for marketing radio equipment⁽¹⁶³⁾. This directive sets health and safety requirements, electromagnetic compatibility, and the efficient use of the radio spectrum. Interestingly, the directive also regulates some other aspects such as privacy and personal data protection, and measures against fraud. Further regulated matters include interoperability, access to emergency services, and compliance regarding the combination of radio equipment and software. According to the RED, ‘radio equipment’ means an ‘electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product

⁽¹⁵⁶⁾ EUIPO EUROPOL IP Crime Threat Assessment Report 2019 : ‘The extent of online piracy is expected to continue increasing in the future. As streaming devices become increasingly integrated, illegal content can be accessed more easily through applications using legitimate technology, such as smart televisions, instead of through illegal streaming devices’.

⁽¹⁵⁷⁾ See discussion *supra*, Section 2.1.

⁽¹⁵⁸⁾ Directive 2004/48/EC, Article 9(1)(b).

⁽¹⁵⁹⁾ Council Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights, OJ L 196, 2.8.2003, p. 7–14.

⁽¹⁶⁰⁾ See Case C-527/15 *Stichting Brein v Wullems (t/a Filmspeler)*, discussed *supra*, Section 1.4.3.2.

⁽¹⁶¹⁾ See discussion in Section 2.3.

⁽¹⁶²⁾ Electrical Safety first (www.electricalsafetyfirst.org.uk, 15-11-2017, ‘Illicit Streaming Devices Pose Electrical and Fire Risk to Users’; FACT (www.fact-uk.org), 16-11-2017.

⁽¹⁶³⁾ Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination’⁽¹⁶⁴⁾.

Arguably, this definition may apply to IPTV devices, insofar as they emit or receive radio waves (for instance by using Wi-Fi/WLAN, bluetooth or other electronic communication protocols). In this respect, ‘vanilla’ devices must fulfil the requirements laid down by the RED and other national regulations in Member States⁽¹⁶⁵⁾. These regulations require that ‘radio equipment’ be subject to a conformity assessment procedure and should carry technical documentation⁽¹⁶⁶⁾. In addition, such equipment should carry a declaration of conformity, and affix the CE marking to the product⁽¹⁶⁷⁾. The name, trade mark and address of the manufacturer should also be displayed on the product, including a serial number or other identification. Importantly, according to the 2017 UK Regulations the manufacturer of such equipment must also cooperate with the enforcing authorities and provide them information upon requests⁽¹⁶⁸⁾. All the above is particularly relevant for enforcement against actors of business models based on resale and import of IPTV streaming devices, particularly at customs level. Accordingly, the EU enforcement framework for products safety includes a specific customs procedure to prevent incompliant goods from entering the Union market. The lack of consistency of the required certifications, marks, labels or information on producer or trader calls the Customs to block the goods at the border and to start a fast notification procedure to the market surveillance authorities in the Member State.

⁽¹⁶⁴⁾ Ibid, Article 2.1(1).

⁽¹⁶⁵⁾ For example, in the UK, the Radio Equipment regulations 2017.

⁽¹⁶⁶⁾ Ibid, Reg. 6-9.

⁽¹⁶⁷⁾ Ibid, Reg. 12-14.

⁽¹⁶⁸⁾ Ibid, Reg. 16.

5. SELECTED JURISPRUDENCE OF MEMBER STATES

This section reviews a selection of judicial decisions in EU Members States having an impact on the illegal IPTV ecosystem, as described in section 2.

5.1 CIVIL CASE LAW AGAINST DIRECT INFRINGERS

5.1.1 *Standing to sue*

The Enforcement Directive requires Member States to recognise specific subjects as persons entitled to seek applications of the enforcement measures, procedures and remedies provided for by law. These include rights holders, licensees, collective management organisations and professional defence bodies⁽¹⁶⁹⁾. However, these persons are only entitled to seek the application of enforcement measures as long as this is permitted by, and in accordance with, national law. This leaves room for some inconsistency across Member States. Specifically, claimants in an action for IPTV infringement may lose standing to sue because the alleged infringement does not fall within the scope of their licence, or because they are not entitled to sue by operation of law. The following cases illustrate these points.

District Court of Mannheim, 8 May 2015 (Germany)⁽¹⁷⁰⁾

The Mannheim Regional Court ruled in May 2015 that a television station that has acquired the broadcasting rights to a football game for cable, satellite and terrestrial broadcasting cannot prohibit a restaurant from receiving the football match via IPTV and publicly show it.

The court rejected the lawsuit since the claimant was not entitled to claim for damages and consequential damages⁽¹⁷¹⁾. The defendant may indeed have broadcasted the base signal in his restaurant but did not violate any rights of the TV station. The court found that that the broadcaster could not conclusively state that it has acquired the exclusive rights to use the TV signal also for transmission via IPTV. The station had relied on a judgment of the district court of Cologne from the year 2011, which, however, in the view of the Mannheim court, only shows that the broadcaster has the rights to broadcast via cable and satellite⁽¹⁷²⁾.

⁽¹⁶⁹⁾ Directive 2004/48/EC, Article 4.

⁽¹⁷⁰⁾ District Court Mannheim, 08 May 2015, 7 O 166/13.

⁽¹⁷¹⁾ § 97 UrhG i.V. with § 15 para. 1, para. 2 No 1, § 19 para. 4 UrhG.

⁽¹⁷²⁾ Decision of the District Court Mannheim, 08 May 2015, 7 O 166/13.

Kopioisto v Telia Finland Oyj, Market Court, 18 June 2019 (Finland) ⁽¹⁷³⁾

In this case (discussed on another ground in the next section), the Finnish Market Court found that the collecting society Kopioisto, which represents authors and performers in the audiovisual sector in Finland, did not have standing to sue an internet service provider for unauthorised retransmission of a TV signal. To bring an infringement claim, the collecting society should be expressly empowered by the rights holders. Citing in support the CJEU decision in *SNB-REACT* ⁽¹⁷⁴⁾, the Court found that Finnish law does not recognise Kopioisto as having the right to apply for the measures provided for in the Enforcement Directive, and EU law leaves the question of standing to sue to national legislation.

5.1.2 *Retransmission of TV signal via internet live streaming*

National courts have decided a number of cases of retransmission of a TV signal over the internet, both from freely available TV broadcasts and from Pay TV channels ⁽¹⁷⁵⁾.

Stichting Brein v Leaper, District court Limburg, 9 May 2018 (Netherlands) ⁽¹⁷⁶⁾

Leaper owns a number of websites where it offers upon subscription access to more than 4 000 TV stations. Sued by the collecting society Stichting Brein, it claims to be a mere intermediary where the choice to access the 'illegal' content belongs entirely to its customers. The court, arguing the flexibility of Dutch copyright law in determining the ways to perform a communication to the public (Article 12 of the Dutch Copyright Act, implementing Article 3 of the Information Society Directive) found Leaper infringing.

Playmédia v France Télévisions, Court of Appeal of Paris, 2 February 2016 (France) ⁽¹⁷⁷⁾

This case is particularly interesting for the argument put by the defence. A streaming website (*playtv.fr*) webcasts free-to-air television broadcasts by — among others — France Télévision (the main national broadcaster) who sued the operators of the website for copyright infringement. In the first degree, defendants argued that not only they did not infringe broadcaster's copyright, but they were obliged to retransmit the signal under the 'must carry' obligation (cable retransmission of a broadcasting signal on the same territory) ⁽¹⁷⁸⁾. The argument however did not convince the court, which ruled against the defendants, both in first and second degree (Appeal).

The case was brought also before the State Council (Conseil d'état), which in turn referred the question to the CJEU, as to whether a Member State could expand the 'must carry' obligation as to include

⁽¹⁷³⁾ *Kopioisto r.y Telia Finland Oyj*, MAO:285/19.

⁽¹⁷⁴⁾ Case C-521/17 *Coöperatieve Vereniging SNB-REACT UA v Deepak Mehta* [2018] E.C.D.R. 23, § 34.

⁽¹⁷⁵⁾ See discussion on *TV Catchup 1*, supra, Section 1.4.2.

⁽¹⁷⁶⁾ *Stichting Brein v Leaper Beheer BV* (also active as 'Flickstore', 'Dump Die Deal' and 'Live TV Store') District court Limburg 9 May 2018 C/03/233371 / HA ZA 17-158 ECLI:NL:RBLIM:2018:4395.

⁽¹⁷⁷⁾ *Playmédia v France Télévisions* Cour d'appel de Paris (pôle 5, ch. 1), 2 février 2016.

⁽¹⁷⁸⁾ Article 34 de la Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard). See Universal Service Directive (2002/22/CE), Article 31.

internet rebroadcasting. On 13 December 2018 the CJEU ruled in the affirmative⁽¹⁷⁹⁾. In France, the Loi L  otard extends the ‘must carry’ obligation to internet broadcasting (webcasting). The *Playmedia* case was subsequently sent before the Supreme Court (Cour de Cassation), which had also referred the question to the CJEU. The Supreme Court eventually rejected Playmedia’s request, siding with France T  l  visions⁽¹⁸⁰⁾.

Kopiosto v Telia Finland Oyj, Market Court, 18 June 2019 (Finland)⁽¹⁸¹⁾

The collecting society Kopiosto sued an internet service provider (Telia) which was broadcasting on the internet some TV channels from Finnish television. Some of these channels were subject to the must carry obligation, and therefore were not subject to copyright infringement claims. Some other TV stations, however, were not subject to the same obligation. For both categories of channels, the court was required to define whether Telia’s activities could be defined as ‘retransmission’. The court rejected the claim that the signal was a retransmission, on the ground that the signal was transmitted directly to Telia without previous communication to the public.

Interestingly, the decision of the Finnish court is consistent with the provision on ‘direct injection’ that will enter into force with the new directive on online broadcast transmission⁽¹⁸²⁾.

5.1.3 Hyperlinking to infringing IPTV

Hyperlinks aggregators are part of the Illegal IPTV ecosystem; they offer on their web pages a collection of hyperlinks to potentially infringing websites or cyberlockers, and/or embedded links to freely available legitimate IPTV services, without the authorisation of the rights holders. A number of cases on hyperlinking have been decided by national courts, some of which have direct relevance for illegal IPTV. In France⁽¹⁸³⁾, Italy⁽¹⁸⁴⁾, and Spain⁽¹⁸⁵⁾ cases were brought against Rojadirecta, an aggregator which provides hyperlinks to live streaming of sporting events originally screened by broadcasters all over the world. The defendant’s claim to be a hosting service protected by Article 14 of the e-commerce Directive was not accepted by any of these courts. Since Rojadirecta provides sports calendars, hyperlinks organisation by subject, and technical instructions on how to install playing software, it was considered an editorial business rather than mere hosting. Consequently, it was held liable to contributory copyright infringement under the applicable national law.

⁽¹⁷⁹⁾ Case C-298/17 *France T  l  visions SA v Playm  dia and Conseil sup  rieur de l’audiovisuel (CSA)*.

⁽¹⁸⁰⁾ Arr  t n  640 du 4 juillet 2019 (16-13.092) — Cour de cassation — Premi  re chambre civile — ECLI:FR:CCASS:2019:C100640.

⁽¹⁸¹⁾ *Kopiosto r.y Telia Finland Oyj*, MAO:285/19.

⁽¹⁸²⁾ Directive (EU) 2019/789, Article 8. See discussion supra, section 1.5.3.

⁽¹⁸³⁾ 19 mars 2015 Tribunal de Grande Instance de Paris, *Ligue de Football Professionnel v. Puerto 80 (Rojadirecta)*.

⁽¹⁸⁴⁾ 17/8/2011, Tribunale Civile di Roma, *RTI c. Rojadirecta*.

⁽¹⁸⁵⁾ A Coru  a Provincial Court (4th Section), PUERTO 80 PROJECTS, S.L.U. (Defendant). V. DTS DISTRIBUIDORA DE TELEVISION DIGITAL S.A. (Claimant), December 28th, 2018 / Case n. 434/2018, Rec. n. 225/2017.

A similar argument was used in Italy against the aggregator *break.com*⁽¹⁸⁶⁾. In this case, the defence of passive hosting was rejected because Break behaves as a content provider, by selecting, organising, optimising and commercially exploiting the content. The Court found the defendant liable of contributory infringement ('contributo agevolatore').

It must be noted that, further to the CJEU decision in *GS Media*⁽¹⁸⁷⁾, activities such as those discussed in the *Rojadirecta* cases and in the *break.com* case may amount to direct copyright infringement (communication to the public). The following two cases illustrate how national courts have applied the CJEU jurisprudence on hyperlinking in the context of illegal IPTV.

Livemovies.gr, Athens Court of Appeal, April 2017 (Greece)⁽¹⁸⁸⁾

The Athens Court of Appeal found that the website *livemovies.gr*, which provided links to infringing materials (movies published online without the authorisation of the rights holders), could not be found liable under *Svensson*⁽¹⁸⁹⁾, since the material was accessible to the whole internet public (albeit without the authorisation of the rights holders). It needs to be noted that the first-degree ruling (2014) preceded the CJEU ruling in *GS Media*⁽¹⁹⁰⁾. However, even in appeal (2017) the website succeeded in declaring its ignorance of the unauthorised content. As per *GS Media* knowledge is presumed in the presence of financial gain, but Livemovies offered its service free of charge.

MyP2P v Premier League, Court of Appeal 's-Hertogenbosch, 17 October 2017 (Netherlands)⁽¹⁹¹⁾

In the Netherlands the Football Association Premier League (UK) sued a platform, MyP2P, which allowed users to stream their own TV content (both freely available and on subscription) to be watched by other MyP2P subscribers. In the Appeal, after *GS Media*, the Court confirmed MyP2P directly infringing because a) it facilitates access to content that Premier League did not consider with the original broadcasts (new public); b) it gave access to content without the authorisation of the rights holder; and c) its knowledge was presumed by the for-profit 'motive' of MyP2P. The platform does not require subscription and does not display advertisement, but its users are offered the possibility to make a donation.

This jurisprudential trend is also confirmed by a Swedish ruling, in which a content licensor, C More Entertainment, sued a person who was providing hyperlinks to ice hockey matches⁽¹⁹²⁾.

⁽¹⁸⁶⁾ Tribunale civile di Roma, 24716, 15 Marzo 2016 (*RTI c. TMFT Enterprises, LLC — Break Media*).

⁽¹⁸⁷⁾ Case C-160/15 *GS Media v Sanoma Media NL*. See discussion supra, sec. 2.4.3.

⁽¹⁸⁸⁾ 1909/2017 Athens Court of Appeal Operator of website www.livemovies.gr against AEPI.

⁽¹⁸⁹⁾ Case C-466/12 *Svensson v Retriever*.

⁽¹⁹⁰⁾ Case C-160/15 *GS Media v Sanoma Media NL*.

⁽¹⁹¹⁾ *MyP2P BV v The Football Association Premier League Limited BV e.a.*, Court of Appeal 's-Hertogenbosch, 17 October 2017, No 200.149.632/02 ECLI:NL:GHSHE:2017:4524.

⁽¹⁹²⁾ NJA 2015 s. 1097 Supreme Court C More Entertainment AB, v. Linus Sandberg.

5.1.4 Illicit IPTV devices

A special case of infringing hyperlinking is the provision of illicit IPTV devices such as fully-loaded set-top boxes, which was considered by the CJEU in *Filmspeler*⁽¹⁹³⁾. After this CJEU ruling, the referring Court of Midden Netherland found *Filmspeler* infringing⁽¹⁹⁴⁾. Moreover, this legal course was confirmed in following cases, as for example *Mediastreamers*⁽¹⁹⁵⁾ and *Moviestreamer*.

Stichting Brein v Moviestreamer, District Court Midden-Nederland 27 October 2017 (Netherlands)⁽¹⁹⁶⁾

This case involved the sale of software that allows one to watch a large range of channels in an easy and fully automated way. Although the court in this case discusses the provision of hyperlinks, it is interesting to note that this business model seems closer to the provision of a fully loaded set-top-boxes rather than to an Aggregator. The software offered for sale by *Moviestreamer* is sold one off (no need for subscription). *Moviestreamer* attempted to deploy a common defence strategy, by claiming to be a 'neutral' intermediary, as the infringing hyperlinks are provided by a third party. However, the judges argued that the links are to content made available without the authorisation of the rights holders and that *Moviestreamer* was aware of the infringing activity, as its business model is for profit (both conditions required by *GS Media*) and therefore ruled against the defendant.

After *Filmspeler*, the liability of sellers and resellers of fully-loaded set-top-boxes is widely accepted by courts. A series of cases leading to criminal convictions have been brought against sellers of illicit IPTV devices in the Czech Republic, Denmark, and the UK. They will be discussed extensively in section 5.3.

5.2 INJUNCTIONS AGAINST INTERNET INTERMEDIARIES

Legal injunctions against internet intermediaries are available in all Member States, to various extents and degrees. They are actionable by either the copyright owner, or the licensor, or a collecting society⁽¹⁹⁷⁾. They can be requested both against the direct infringer or the intermediary, depending on the type of measure. Investigative injunctions (evidence preservation seizures, temporary measures) are available against the direct infringers in every jurisdiction.

⁽¹⁹³⁾ C-527/15 *Stichting Brein v Wullems (t/a Filmspeler)*.

⁽¹⁹⁴⁾ 10 June 2015, Court Midden-Nederland, *Stichting Brein v Filmspeler*, ECLI:NL:RBMNE:2015:4343 C/16/372666 / HL ZA 14-204.

⁽¹⁹⁵⁾ 2 December 2015, District court Midden-Nederland, *Stichting Brein v [defendant]*, ECLI:NL:RBMNE:2015:8685 C/16/400002 / KG ZA 15-675.

⁽¹⁹⁶⁾ *Stichting Brein v Moviestreamer International BV*, District court Midden-Nederland (summary proceedings) 27 October 2017 C/16/442373 / KG ZA 17-518 ECLI:NL:RBMNE:2017:5510.

⁽¹⁹⁷⁾ These elements vary across EU jurisdictions, see F. Petillion (ed) *Enforcement of Intellectual Property Rights in the EU Member states* (Intersentia 2019 Antwerpen) at 15.

Injunctions are normally granted by judicial authorities, with the notable exception of Italy where the communications authority (AGCOM) has the power to grant injunctions to block access to websites hosting allegedly infringing material by means of an administrative procedure⁽¹⁹⁸⁾.

5.2.1 Live blocking injunctions against network providers

Blocking injunctions to stop access to an infringing website are requested against internet access providers. The most effective and most important against illegal IPTV covering live events are ‘live’ injunctions, that require blocking a streaming flow for the duration of the protected content (normally a sports event). There is evidence of this practice in France, Italy, Netherlands⁽¹⁹⁹⁾ and the UK⁽²⁰⁰⁾. The conditions requested by courts to grant such injunctions have been discussed in the following case:

Football Association Premier League v BT, High Court, 8 March 2017 (UK)⁽²⁰¹⁾

The Premier League applied for blocking injunctions against the six main retail network service providers on the basis of s.97A of the UK’s Copyright, Designs and Patents Act 1988 (the 1988 Act), which implemented Article 8(3) of the Information Society Directive. This is the first case in England of a ‘live’ injunction, because the providers were required to block access to a specific sports event and only for its duration. Importantly, according to s.97A the court has the power ‘to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright’. Therefore, four criteria need to be satisfied to obtain the injunction: a) the defendant has to be a service provider; b) the users and/or the operators of the blocked websites infringe rights holders’ copyrights; c) these users and operators use the network services targeted by the injunction in order to infringe copyright; d) that the service provider has actual knowledge of this.

All these requirements were met by the case at hand, according to evidence presented by the claimant. Premier League presented evidence of large volumes of internet traffic on at least three of network service providers in correspondence with major sports events. Moreover, correspondence between Premier League and the service providers was produced to indicate repeated communication of the infringement prior to the request of the injunction.

⁽¹⁹⁸⁾ See supra, sec. 5.4.

⁽¹⁹⁹⁾ 02/11/2017 Jugement au fond en la forme des référés (Article L. 336-2 CPI) Blocage: effet 12 mois - 15/12/2017; Jugement au fond en la forme des référés (Article L. 336-2 CPI)- Blocage et déréférencement effet 12 mois - 25/05/2018; Jugement au fond en la forme des référés (Article L. 336-2 CPI)- Blocage et déréférencement: effet 12 mois - 14/12/2018 (RG 18/10652); Jugement au fond en la forme des référés Article L. 336-2 CPI) - Blocage et déréférencement: effet 12 mois- 29/06/2013; Tribunale di Milano Blocking injunctions on ISP (*Rojadirecta*) 24 January 2018C/09/485400 / HA ZA 15-367 ECLI:NL:RBDHA:2018:615; Court the Hague, *The Football Association Premier League v Ecatel*; 28 April 2015.

⁽²⁰⁰⁾ *Twentieth Century Fox Film Corporation and Others v Sky UK Ltd and Others* [2015] EWHC (Ch) 1082 (‘Popcorn Time case’); *Football Association Premier League Ltd v British Telecommunications Plc & Ors* [2017] EWHC 480 (Ch); (‘FAPL v BT 1’); *Football Association Premier League Ltd v British Telecommunications Plc* [2018] EWHC 1828 (Ch); (‘FAPL v BT II’); *UEFA v BT* [2018] EWHC 1900 (Ch); *Matchroom Boxing Ltd v BT Plc* [2018] EWHC 2443 (Ch).

⁽²⁰¹⁾ *Football Association Premier League Ltd v British Telecommunications Plc & Ors* [2017] EWHC 480 (Ch).

Live blocking injunctions in connection to sporting events have been granted in at least three other cases in the UK: two of them in relation to football matches from Premier League and UEFA respectively ⁽²⁰²⁾, and one in connection with a single major boxing match ⁽²⁰³⁾.

5.2.2 Injunctions against search engines and social media

De-listing injunctions are orders directed to search engines to remove an URL address from the search results. While such orders can be granted by courts, de-listing (or de-indexing) can normally be requested directly to the search engine as part of their take down policy. There is evidence of this type of injunction in France, where several collecting societies have requested and obtained from the Court of Paris (3rd Chamber) a number of injunctions to the principal network service providers to block a number of IPTV infringing websites. Interestingly, they were also granted a de-listing injunction to Google to delete these websites from its search results ⁽²⁰⁴⁾

As discussed in section 2, exposure on social media is part of the strategy to promote unauthorised IPTV services. In this connection, injunctions to remove information from social media platforms are an important enforcement tool for rights holders, as illustrated by the following case.

RTI v Facebook, Civil Court of Rome, 15 February 2019 (Italy) ⁽²⁰⁵⁾

Facebook hosted a page with offensive content against a performer in a TV show broadcasted by RTI (Reti Televisive Italiane) and hyperlinks to broadcast were made available on YouTube without the consent of RTI.

The court referred to *Filmspeler* to conclude that hyperlinking amounted to communication to the public (making available). On the hosting exemption, the court observed that: a) the service acquired knowledge (although *ex post*) of the illicit nature of the information; the notice served by RTI was sufficiently detailed, despite the absence of the URLs; b) Facebook delayed the removal of the information ('inerzia protratta'): two years later, the content was still available. In this instance, the court found it unnecessary to address the issue of whether the hosting service was 'active' or 'passive', and condemned Facebook to pay damages, both to RTI and to the actresses performing in the series, and ordered the social media giant to stop future violations on the same content.

⁽²⁰²⁾ *Football Association Premier League Ltd v British Telecommunications Plc* [2018] EWHC 1828 (Ch.) and *UEFA v BT Plc* [2018] EWHC 1900 (Ch.).

⁽²⁰³⁾ *Matchroom Boxing Ltd v BT Plc* [2018] EWHC 2443 (Ch.).

⁽²⁰⁴⁾ 02/11/2017 Jugement au fond en la forme des référés (Article L. 336-2 CPI)- Blocage : effet 12 mois - 15/12/2017; Jugement au fond en la forme des référés (Article L. 336-2 CPI)- Blocage et déréférencement effet 12 mois - 25/05/2018; Jugement au fond en la forme des référés (Article L. 336-2 CPI)- Blocage et déréférencement: effet 12 mois - 14/12/2018 (RG 18/10652); Jugement au fond en la forme des référés (Article L. 336-2 CPI)- Blocage et déréférencement: effet 12 mois- 29/06/2013.

⁽²⁰⁵⁾ RTI c. Facebook, Tribunale civile di Roma, 15 February 2019.

5.2.3 Injunctions against streaming servers

Streaming service providers may include services that rent space on their servers to host the streaming websites, as well as services that cover the technical components required for the delivery of audiovisual content⁽²⁰⁶⁾. Depending on the activity performed, they may or may not fall within the definition of ‘hosting’ of Article 14 of the e-Commerce Directive⁽²⁰⁷⁾.

Reportedly, rights holders try to stop these services from hosting unauthorised content (or links to unauthorised content) via legal notices. Failing to respond to notice may trigger liability if the rights holder can demonstrate that the activity of the service falls within the scope of Article 14. Some jurisprudence has been retrieved within this study on this type of case scenario. For example, in Italy a formal blocking injunction (executive order) was denied, alleging the ‘neutrality’ of a service home to a number of infringing websites (Worldstream)⁽²⁰⁸⁾, but it was granted on two occasions one year later (*RTI c Worldstream; RTI c Choopa*)⁽²⁰⁹⁾.

In the Netherlands, this type of hosting intermediary was found infringing in the *Ecatel* case.

Football Association Premier League v Ecatel, Court of The Hague, 28 April 2015 (Netherland)⁽²¹⁰⁾

Ecatel is a Dutch service provider that offers the rental of ‘dedicated servers’. These allow subscribers of the service to access football matches also beyond the Netherlands. The UK Premier League, which owns the rights to broadcast these matches, brought summary action against Ecatel in 2014 and won. In 2015, Ecatel brought in turn summary action against Premier League, claiming to be a mere server rental service and not an hosting provider in the sense of Article 14 of the e-Commerce Directive. At that stage, the court accepted this argument. Premier League brought another lawsuit before the court of The Hague and in 2018 won against Ecatel. Interestingly, in this case the court argued that a) sports events are protected by copyright insofar as creative choices are made (which include the live commentary); b) that the absence of the fixation requirement (necessary under English law to grant copyright protection but not under Dutch law) was not relevant. But in any event, the court added that, given the nature of live broadcasts, ‘the fixation arises at the same time as the work is created’. Finally, the court granted in this case a ‘live’ injunction to Premier League, which obliged Ecatel to block access to the streaming originating from its servers on the occasion and for the duration of specific streaming events.

This position of the Dutch court in favour of the liability of hosting providers was confirmed in a summary proceeding against Global Layer, another server which was ordered to block a specific website

⁽²⁰⁶⁾ See supra, sec. 3.4.2.

⁽²⁰⁷⁾ See supra, sec.5.1.2.

⁽²⁰⁸⁾ Tribunale di Roma 26-10-2011 RTI v Worldstream; Tribunale di Roma 20-10-2012 RTI v Choopa.

⁽²⁰⁹⁾ Tribunale di Roma 14-12-2012 executive injunction (ordinanza esecutiva) against Worldstream to block access to ‘Webcaston’ streaming sports matches.

⁽²¹⁰⁾ Court the Hague, *The Football Association Premier League v Ecatel*; 28 April 2015.

(04stream.com) which was making available several live streaming of live football events⁽²¹¹⁾. In this case, the injunction was not ‘live’ (not related to a specific event) but it was directed at the whole website.

5.2.4 Disclosure of information

Internet intermediaries can be requested to disclose information for the purpose of prosecuting an alleged infringement. There are reports of requests in this sense repeatedly granted, for example in Cyprus, where two plaintiffs have requested information on alleged copyright infringers offering illegal IPTV services online to the relevant internet service provider. The request was granted and confirmed in all degrees of justice up to the Supreme Court⁽²¹²⁾.

5.3 CRIMINAL CASE LAW

To date, criminal prosecutions against actors involved in illegal IPTV have been brought in at least four Member States: Denmark, Czech Republic, France and United Kingdom. All three business models discussed in section 2 — business-to-consumer, business-to-business and free streaming portal —⁽²¹³⁾ seem to have been the target of criminal prosecution.

5.3.1 Hyperlinking cases in the Czech Republic and France

Criminal cases on hyperlinking were discussed in the Czech Republic and in France.

In the first case the defendant administered internet pages including embedded links to the websites *zkouknito.cz* and *ulozto.cz*, which offered unauthorised access to pay-tv. The case reached the Supreme Court, which ruled irrelevant the fact that the defendant did not himself publish online the protected content. The mere fact of providing embedded links to websites which, in turn, provide unauthorised access to protected content makes his acts unlawful. The Court specified that this is indeed an act of communication to the public and it infringes copyright law, therefore, the defendant was sentenced to conditional imprisonment for 3 years.⁽²¹⁴⁾

In another case a teenager (nicknamed ‘tulip’) offered hyperlinks to content stored on external servers by embedding it in his website. He was found infringing, but the sentence was suspended⁽²¹⁵⁾. Similarly, in France, a high school student built a live-streaming platform (ArTV) which became

⁽²¹¹⁾ N.V. Ado Den Haag et al. v Global Layer BV (04stream.com), Summary proceedings Court the Hague 17 August 2016 C/09/515172 / KG ZA 16-905 ECLI:NL:RBDHA:2016:9685.

⁽²¹²⁾ Ioannis Hatzioannou, Court of Nicosia, 23 April 2018; Ioannis Chatziioannou and George Longkrits, Supreme Court of Cyprus, 2 May 2018; Ioannis Hatzioannou and George Longkrits, Supreme Court of Cyprus, 10 July 2018.

⁽²¹³⁾ *Supra*, sec. 3.1.

⁽²¹⁴⁾ 29.5.2013 Supreme Court 5 Tdo 271/2013 ‘ulozto.cz’

⁽²¹⁵⁾ Supreme Court 27.2.2013 8 Tdo 137/2013 ‘Liberec Pirate’ CZ: NS :2013: 8.TDO.137.2013.1.

increasingly popular, especially with French nationals resident abroad⁽²¹⁶⁾. Reportedly, he was arrested by the police but subsequently released, and the platform dismantled.

5.3.2 Illicit IPTV and cardsharing in Denmark

One of the first cases to deal with the specific technical modalities of illegal IPTV was brought in Denmark in 2015, where a website of Illegal streaming run by a private individual was pursued by the Danish State Prosecutor for Serious Economic and International Crime (SØIK) over a notice by Nordic Content Protection⁽²¹⁷⁾. The site *whargarbl.dk* provided unlicensed streaming of 80 TV channels, and the court convicted the defendant to a 60-day suspended sentence and DKK 100 000 in damages. A similar outcome was reached in a case involving the streaming website *floppi.org*, which generated huge internet traffic between 2014 and 2015. In October 2015, the defendant received 8 months suspended sentence⁽²¹⁸⁾. One of the most complex cases heard by criminal courts is *Cardpro*, a scenario involving multiple actors and techniques.

Cardpro Næstved District Court, 30 March 2017 (Denmark)

The case involved two Danish nationals engaged in making TV content available on a large scale through illegal card-sharing (or sharing satellite TV codes via internet), IPTV and on-demand streaming via internet. The first defendant provided internet connection and space for hardware; the second defendant helped run the operation, set up equipment and collected payments from customers. A third individual based in Thailand managed the operation and received payments. The service operated by the defendants, *Cardpro*, gave customers access to 102 satellite TV channels via illegal card-sharing and 39 IPTV channels via the internet. In addition, *Cardpro* illegally made available on-demand content including films, cartoons and TV series. The prosecutors, assisted by Nordic Content Protection (NCP), argued that the provision of IPTV and on-demand streaming services infringed the Copyright Act (rights of communication to the public and making available), whereas card-sharing entailed a violation of the Radio and Television Act (section 91) — which prohibits, inter alia, the selling, owning or modifying of decoding equipment with the purpose of providing unauthorised access to encoded radio or television broadcasts. Additionally, the prosecutors requested application of Danish Criminal Code, sec. 299b(1) and (6), since the violations were particularly serious and committed intentionally and under ‘particularly aggravating circumstances’.

On 30 March 2017, the District Court found both defendants guilty of violating both the Copyright Act and the Radio and Television Act. The Court found only the second defendant guilty of violating the Criminal Code. As a consequence, the first defendant was sentenced to a 30-day suspended prison term conditional upon a one-year probationary period and 40 hours community service and the second

⁽²¹⁶⁾ Brossat, T. ‘Vincent, 17 ans, lycéen, et créateur d’un des sites les plus populaires de streaming illégal’, *Le Monde*, 20-10-2018 (accessed 14-06-2019).

⁽²¹⁷⁾ April 2015, Danish State Prosecutor for Serious Economic and International Crime (SØIK) *Retten i Aalborg v. Private individual (Streaming site whargarbl.dk)*.

⁽²¹⁸⁾ October 2015, Danish State Prosecutor for Serious Economic and International Crime (SØIK) *Retten i Næstved v. Private individual (Streaming site floppi.org)*.

defendant received a 5-month suspended prison term conditional upon a one-year probationary period and 100 hours community service

The second defendant appealed the judgment. The Eastern High Court issued its judgment on 3 December 2018, in which it upheld the District Court judgment.

Another two cases were reported in Denmark where the defendants sold set-top-boxes allowing access to a large number of IPTV channels without the authorisation of the rights holders; they both led to criminal convictions and suspended sentences⁽²¹⁹⁾.

5.3.3 *Illicit IPTV devices in the United Kingdom*

Although the applicable law varies from case to case, there are a wide range of provisions which have been applied in the UK to the sale, advertising, supply or use of set-top boxes for illicit streaming. These include the provisions of the Copyright, Designs and Patent Act 1988 on fraudulent reception of transmission⁽²²⁰⁾ and on circumvention of technological measure⁽²²¹⁾ 296ZB, but also the provisions of the Fraud Act 2006 on possession, making and/or supply of articles for use in frauds⁽²²²⁾. Under those provisions, an individual commits an offence by supplying set-top boxes (both fully loaded or ‘vanilla’) having knowledge that that they would be used illegally. Additionally, the supplier of set-top boxes can commit the offence of running a fraudulent business.

Moreover, the common law offence of conspiracy to defraud and the inchoate offence of encouraging or assisting crime (which may involve any of the statutory offences mentioned above), coupled with the relevant provisions of the Serious Crime Act 2007, have assisted the prosecutors in dealing with illegal IPTV cases. In this connection, prosecutors have secured serious crime prevention orders against defendants, which make the repeated offender not only liable to further prosecution, but also in contempt of a court order.

An example of conviction under the common law offence of conspiracy to defraud is a prosecution on behalf of Premier League and FACT (the Federation Against Copyright Theft) at Nottingham Crown Court in 2016⁽²²³⁾. The defendants in this case supplied devices and services to pubs and individuals that facilitated the viewing of pay-tv without appropriate payment to the broadcasters. The charge against the defendants was that they conspired together to defraud the broadcasters of pay-tv services, the Premier League and other persons having an interest in the content of pay-tv⁽²²⁴⁾. The

⁽²¹⁹⁾ *Københavns Byret (Copenhagen City Court) v. Private individual* December 2016 and *Østre Landsret* 2017 (see *Nordic Content Protection Case Studies 2018*).

⁽²²⁰⁾ Copyright, Designs and Patents Act 1998, section 297 (offence of fraudulently receiving programmes) and 297A (unauthorised decoders).

⁽²²¹⁾ *Ibid.*, section 296ZB (devices and services designed to circumvent technological measures).

⁽²²²⁾ Fraud Act 2006, sections 6 (possession of articles for use in fraud), 7 (making or supplying articles for use in frauds) and 11 (obtaining services dishonestly).

⁽²²³⁾ *R v W.O. and T.O.*, Nottingham Crown Court, 9 December 2016 (unreported).

⁽²²⁴⁾ *Illicit IPTV Streaming Devices — Call for Views* (UK Intellectual Property Office, 2007), p. 2.

first defendant was sentenced to 4 years in prison and the second one received a 2-year suspended prison sentence.

On the same day, the Crown Prosecution Service and the Police Intellectual Property Crime Unit (PIPCU) obtained a conviction under the Serious Crime Act 2007 against an individual who commercialised illegal IPTV devices⁽²²⁵⁾. The defendant had placed for sale on an eBay account, IPTV receivers, with a description suggesting that the devices can stream a large number of unauthorised channels. Although no add-ons were found on the set-top-boxes seized on the premises, the individual was charged for an ‘act capable of encouraging or assisting the commission of an offence’. Applying section 11 of the Fraud Act 2006, the individual was found to ‘dishonestly and knowingly obtaining services from SKY without the authority of SKY and without paying the required subscription fee to SKY’⁽²²⁶⁾. The defendant pleaded guilty and was sentenced to a fine of GBP 392 and a victim surcharge of GBP 39, along with a contribution to prosecution costs⁽²²⁷⁾.

Interestingly, criminal prosecution may succeed also against suppliers of ‘vanilla’ devices (namely devices that are not yet configured to receive illegal streaming) if the circumstances suggest that the supplier intends to assist the customers in committing the offence. This is illustrated in the following case:

R v M.M., Teesside Crown Court, 6 March 2017 (UK)

Defendant sold IPTV boxes for around GBP 1 000 each to pubs and clubs around the country, targeting those establishments through placing adverts in national magazines such as *The Caterer*, *Licensee* and *Hotelier News*, offering a one-off payment of GBP 995 for ‘UK’s No. 1 Sports System’ including 380 games a season and claimed his devices were ‘100 % legal’

The set-top-boxes provided by the defendant were not illegal, but when they were modified, they could be used to freely view content which was available only on pay-tv. The court applied section 297A of the Copyright, Designs and Patents Act 1988 (distribution of unauthorised decoders). The defendant admitted breaching copyright law by advertising and selling adapted IPTV boxes. He was ordered to pay a total of GBP 250 000 for illegally selling IPTV boxes to pubs and clubs and received a 10-month prison sentence, suspended for 1 year. A Proceeds of Crime Order was also made against him for a further GBP 80 000.

A further prosecution was brought before the same court on behalf of Premier League and FACT in 2017⁽²²⁸⁾. Two individuals were involved in selling fully loaded set-top-boxes in retail stores and online. The first defendant operated a company which sold IPTV boxes from an independent store and online, both directly to consumers and to other businesses for resale, advertising that the IPTV boxes would provide customers with free access to movies, live sports and TV releases. The second defendant

⁽²²⁵⁾ *R v J.R.*, City of London Police, 9 December 2016 (unreported).

⁽²²⁶⁾ IP Crime Illicit IPTV Streaming Devices — Call for Views (UK Intellectual Property Office, 2007), p. 2.

⁽²²⁷⁾ IP Crime and Enforcement. Report 2016/2017 (UK Intellectual Property Office), p. 24.

⁽²²⁸⁾ *R v B.T. and J.A.*, Teesside Crown Court, 20 October 2017 (unreported).

sold IPTV boxes supplied by the first defendant to consumers. They received, respectively, a suspended prison sentence of 21 months and 18 months.

To date, the longest prison sentence for sale of illegal IPTV subscriptions was awarded in a case heard at the Warwick Crown Court in February 2019⁽²²⁹⁾. Reportedly, three individuals trading under Dreambox (unincorporated) sold illegal subscriptions to IPTV packages including Premier League matches to more than 1 000 pubs, clubs and private homes over 10 years of activity. The court found the individuals guilty of conspiracy to defraud and imposed a combined sentence of 17 years.

⁽²²⁹⁾ *R v S.K, P.R. and D.M. (Dreambox)*, Warwick Crown Court, 19 February 2019 (unreported).

6. CONCLUSIONS AND PERSPECTIVES

The illegal IPTV phenomenon is a rising trend in the global market. It is related to both the proliferation of legitimate IPTV services and ease of access to unauthorised IPTV.

This report has been carried out to estimate the number of individuals that consume unauthorised IPTV as well as to assess the potential revenue generated by copyright-infringing IPTV providers. Quantitative estimation is based on official and harmonised data sources in order to ensure full comparability of the reported estimates among the EU Member States. This study also benefits from cooperation with the EUIPO Observatory stakeholders and relies on data and knowledge shared by experts of IPTV market conditions.

Economic analysis provides coherent estimates of the size of the problem of illegal IPTV in terms of number of users and illicit revenue generated:

- The number of users involved in unauthorised IPTV streaming is estimated to be 13.7 million persons⁽²³⁰⁾, corresponding to 3.6 % of the total EU-28 population in 2018.
- Providers of copyright-infringing IPTV subscriptions are estimated to have generated EUR 941.7 million of annual unlawful revenue in 2018.
- A single user on average spent EUR 5.74 per month in 2018 to access unauthorised IPTV online in the EU.

The results of the illegal IPTV assessment provide evidence and act as sound information tool for policymakers, industry and European citizens.

Illegal IPTV takes place in all EU countries even though to a different extent. Subsequently, copyright-infringing IPTV impacts legal TV providers and broadcasters in terms of lost sales, which indirectly might lead to lost jobs and loss of public revenue. Estimates of potential monetary losses caused to business is an important element that can be addressed in future studies.

Against this background, EU law provides broadcasters and other rights holders with extensive copyright protection and a wide range of enforcement measures, which have been the basis of increasing numbers of civil and criminal prosecutions in many Member States. While the wrongdoing of individual actors involved in IPTV crime is often undisputed, the liability of some of the key intermediaries is still unsettled in the jurisprudence and will require further judicial scrutiny.

The study has shown that the delivery of illegal IPTV constitutes a complex ecosystem that supports a variety of business models. These business models evolve quickly, to adapt to changes in technology and customers' expectations, but are relatively stable in their basic structure. Effective enforcement of broadcasting rights online is a challenge that depends on better understanding of the illegal IPTV ecosystem as a whole.

⁽²³⁰⁾ Persons aged 16-74.

BIBLIOGRAPHY

Industry & Stakeholder' Reports

- British Screen Advisory Council (BSAC), Submission (4 April 2017), 'IPO Call for Views on illicit IPTV Streaming Devices' <https://www.bsac.com>
- BT Submission (6 April 2017), 'IPO Call for Views: Illicit IPTV Streaming Devices': — <https://www.btplc.com>
- Cybersecurity unit of Kudelski Group (2016) 'The new face of pay TV piracy and how to fight it'
- Digital Citizens Alliance (2019), 'Fishing in the Piracy Stream: How the Dark Web of Entertainment is Exposing Consumers to Harm', April 2019
- Digital Citizens Alliance (2017): 'Trouble in Our Digital Midst: How Digital Platforms Are Being Overrun by Bad Actors and How the Internet Community Can Beat Them at Their Own Game', June 2017
- Digital Citizens Alliance (2015) 'Good Money Still Going Bad. Digital Thieves and the Hijacking of the Online Ad Business'
- Envisional, January (2011), 'Technical report: An Estimate of Infringing Use of the Internet'
- European Audiovisual Observatory (2016), 'VOD, platforms and OTT: which promotion obligations for European works?' Strasbourg (2016). ISSN 2079-1062
- Frontier Economics (2017): 'The economic impacts of counterfeiting and piracy. Report prepared for BASCAP and INTA', 2017
- Hadopi (2018), 'Study on new strategies of illegal access to content online'
- Hadopi (2017), 'International Survey: Key lessons learned from international benchmarking', July 2017
- Motion Picture Association of America: 'Public comment on the 2017 Special 301 Out of Cycle Review of Notorious Markets. Docket No USTR-2017-0015', 2 October 2017
- MPA Asia-Pacific (2018), 'Promoting and Protecting the Screen Community', Issue Jan — Jun 2018
- Nordic Content Protection (2018) 'Case Studies 2018'
- Nordic Content Protection (2017), 'Illegal distribution and sales of access to television broadcast. Trend Report 2017'
- Sandvine (2017), '2017 Global Internet Phenomena. Spotlight: Subscription Television Piracy', 2017
- Sandvine (2017), '2017 Global Internet Phenomena. Spotlight: The 'fully loaded' Kodi box', 2017
- Sandvine (2016), 'Video and Television Piracy: Ecosystem and Impact', An Industry Whitepaper
- Strategy& PWC (2015), 'Value shifts in the TV and video ecosystem'
- The Industry Trust (2016): 'IPTV Piracy: A study on set-top-box and stick infringement for the industry'

EUIPO Reports

- EPO and EUIPO (2019), 'IPR-intensive industries and economic performance in the European Union'
- EUIPO (2019), '2019 Intellectual Property and Youth Scoreboard'
- EUIPO (2019), 'Status Report on IPR Infringement'
- EUIPO (2018), 'IP Enforcement. Case-law collection on the balance between the right of information and fundamental rights in the European Union', doi:10.2814/36519

- EUIPO (2018), 'Study on Legislative Measures Related to Online IPR Infringements', doi:10.2814/819909
- EUIPO (2018), 'Identification and Analysis of Malware on Selected Suspected Copyright-Infringing Websites', doi: 10.2814/004056
- EUIPO and Europol (2017), '2017 Situation Report on Counterfeiting and Piracy in the European Union'
- EUIPO and Europol (2015), '2015 Situation Report on Counterfeiting in the European Union'
- EUIPO (2017), 'European Citizens and Intellectual Property: Perception, Awareness and Behaviour' Report. Fieldwork: from 21 to 28 October 2016
- EUIPO and OECD (2016), 'Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact' (OECD Publishing, Paris, 2016). Available at: <http://dx.doi.org/10.1787/9789264252653-en>

European Union policy reports

- European Audiovisual Observatory (2016) 'Audiovisual sports rights — between exclusivity and right to information', IRIS Plus 2016-2
- European Audiovisual Observatory (2015) Copyright enforcement online: policies and mechanisms, IRIS Plus 2015-3
- European Commission (2014), 'Estimating displacement rates of copyrighted content in the EU'

Reports by National authorities

- UKIPO (2018): 'Online Copyright Infringement Tracker', Wave 8 (March 2018), Overview and key findings. Research commissioned by the IP office and carried out by Kantar Media, May 2018
- UKIPO (2017), 'Cracking down on digital piracy', Report, September 2017
- UKIPO (2017), 'Government Response to a technical consultation on transitional arrangements following the repeal of section 73 of the Copyright, Designs and Patents Act 1988 (reception and retransmission of wireless broadcast by cable)'
- UKIPO (2016/17), 'IP Crime and Enforcement Report'
- UKIPO (2016), 'Online Copyright Infringement Tracker'. Wave 5 (Covering period March 15 — May 15), Overview and key findings. Research commissioned by the IP office and carried out by: Kantar Media, July 2016
- UKIPO (2016), 'Online Copyright Infringement Tracker', Wave 6, March 16 — May 16, Overview and key findings. Research commissioned by the IP office and carried out by Kantar Media, July 2016
- UKIPO (2016) 'Online Copyright Infringement Tracker', Wave 7, March 16 — May 16, Overview and key findings. Research commissioned by the IP office and carried out by: Kantar Media, June 2016.
- UKIPO (2015/16), 'IP Crime Report'
- UKIPO (2013), 'Online Copyright Infringement Tracker', Wave 3 (Covering period November 12 — January 13). Overview and key findings. Prepared for Ofcom by Kantar Media
- UKIPO (2013), 'Online Copyright Infringement Tracker' Wave 4 (Covering period March 13 — May 13)', Overview and key findings. Prepared for Ofcom By Kantar Media
- UKIPO (2012), 'OCI Tracker Benchmark Study', Q3 2012. Prepared for Ofcom by Kantar Media

UKIPO (2012), 'Online Copyright Infringement Tracker', Wave 2 (Covering period August — October 2012). Overview and key findings, Prepared for Ofcom By Kantar Media

Office of the US Trade Representative (2017): '2017 Out-of-Cycle Review of Notorious Markets'

Legal Literature

- Ainslie, A. (2015) 'The Burden of Protecting Live Sports Telecasts: The Real Time Problem of Live Streaming and App-Based Technology' (December 4, 2015). Available at SSRN: <https://ssrn.com/abstract=2729641>
- Barissat, (2014) L. 'Le streaming, analyse et commentaires de la décision du TGI de Paris du 28 novembre 2013', *Commissions Ouvertes*
- Borghi, M. (2011) 'Chasing Copyright Infringement in the Streaming Landscape', IIC — *International Review of Intellectual Property and Competition Law*, 42(3), 316
- CRS Report for US Congress (2011) 'Illegal Internet Streaming of Copyrighted Content: Legislation in the 112th Congress' at <https://www.everycrsreport.com/reports/R41975.html>
- Giovannella, F. (2017), *Copyright and Information Privacy*, E. Elgar
- Guibault, L. Meltzer, R. (2004) 'The Legal Protection of Broadcast Signals', *IRIS Plus*, Legal Observations of the European Audiovisual Observatory, Issue 2004-10
- Husovec, M. (2017) *Injunctions Against Intermediaries in the European Union*, Cambridge University Press
- Kucsko and Handig (2017) *Urheberrecht*, 2nd ed. Manz Verlag
- Margoni, T. (2016) 'The protection of sports events in the EU: property, intellectual property, unfair competition and special forms of protection', IIC — *International Review of Intellectual Property and Competition Law*, 47(4), 386
- Perrin, S.R. (2017) 'A critical analysis of the effect of copyright infringement on the UK film and cinema industries', LLM thesis, September 2017
- Priest E. (2015) 'Acupressure: the Emerging Role of Market Ordering in Global Copyright Enforcement', *SMU Law Review*, Vol. 68, pp. 169-242
- Schovsbo, Rosenmeier and Petersen (2018) *Immaterialret* (5th edition)
- Synodinou, T. and Jougoux, P. (2017) 'The legal framework governing online service providers in Cyprus' in G. Dinwoodie (ed.), *Secondary Liability of Internet Service Providers*, Springer

Economic — Quantification Studies

- Danaher, B. Smith, M.D. Telang, R. (2014), 'Piracy and Copyright Enforcement Mechanisms', *Innovation Policy and the Economy*, Volume 14, edited by Josh Lerner and Scott Stern, University of Chicago Press. NBER, June 2014
- Danaher B., M. D. Smith and R. Telang (2015): 'Copyright Enforcement in the Digital Age: Empirical Economic Evidence and Conclusions', Advisory Committee on Enforcement, Tenth Session, Geneva, November 23 to 25, 2015, World Intellectual Property Organization
- European Commission (2014) 'Estimating displacement rates of copyrighted content in the EU'
- Frontier Economics (2017), 'The economic impacts of counterfeiting and piracy', Report prepared for BASCAP and INTA

- Liebowitz, S.J (2005). 'Economists Examine File-Sharing and Music Sales', *The Industrial Organization of Digital Goods and Electronic Markets* edited by Illing and Waelbroeck (MIT press, 2005)
- Liebowitz, S.J (2013), 'The impact of internet piracy on sales and revenues of copyright owners', *Handbook on the Digital Creative Economy*, edited by Ruth Towse and Christian Handke, 2013
- Mateus, A.M. and Peha, J.M. (2011), 'Quantifying Global Transfers of Copyrighted Content using BitTorrent', — Carnegie Mellon University. TPRC 2011 — The 39th Research Conference on Communication, Information and Internet Policy
- Smith M. D. and R. Telang (2012): 'Assessing the Academic Literature Regarding the Impact of Media Piracy on Sales', 2012

Computer Science — Technical Literature

- Choyi et al. PATENT: 'Mechanism for identifying illegal IPTV services', 2014
- Dubovskis, V., Teilans, A., and Visocikis, N.: 'IPTV statistic data collection, processing and preparation for use in a modeling system', *Procedia Computer Science* 77 (2015) 221-226
- Ibosiola D., Steery B., Garcia-Recueroy A., Stringhiniz G., Uhligy S., and Tysony G.: 'Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers', 2018
- Yu, G., Westholm, T., Kihl, M., Sedano, I., Aurelius, A., Lagerstedt, C., & Ödling, P. (2009). 'Analysis and characterization of IPTV user behavior'. Paper presented at IEEE Symposium on Broadband Multimedia Systems and Broadcasting, Bilbao, Spain
- Lee, H.J.: 'A Review of IPTV Threats Based on the Value Chain', *KSII Transactions on Internet and Information Systems*, Vol. 3, No 2, April 2009
- Rafique M. Z., Van Goethem T., Joosen W., Huygens C., and Nikiforakisy N.: 'It's Free for a Reason: Exploring the Ecosystem of Free Live Streaming Services', 2016

TABLE OF CASES

CJEU

- C-521/17 *Coöperatieve Vereniging SNB-REACT UA v Deepak Mehta* [2018] E.C.D.R. 23
- C-310/17 *Levola Hengelo BV v Smilde Foods BV* [2019] E.C.D.R. 2
- C-265/16 *VCAST Ltd v RTI SpA*, [2018] E.C.D.R. 5
- C-610/15 *Stichting Brein v Ziggo BV* [2017] E.C.D.R. 19
- C-527/15 *Stichting Brein v Wullems (t/a Filmspeler)* [2017] E.C.D.R. 14
- C-275/15 *ITV Broadcasting Ltd v TV Catchup Ltd* [2017] E.C.D.R. 10 (*TV Catchup 2*)
- C-160/15 *GS Media BV v Sanoma Media Netherlands BV* [2016] E.C.D.R. 26
- C-484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* [2016] E.C.D.R. 26
- C-279/13 *C More Entertainment AB v Linus Sandberg*, [2015] E.C.D.R. 15
- C-348/13 *BestWater v Mebes & Potsch* (unreported)
- C-466/12 *Svensson v Retriever Sverige AB*, [2014] E.C.D.R. 9

- C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH*, [2014] E.C.D.R. 12
- C-607/11 *ITV Broadcasting Ltd v TV Catchup Ltd* [2013] E.C.D.R. 9 (*TV Catchup 1*)
- C-461/10 *Bonnier Audio AB v Perfect Communication Sweden AB* [2012] E.C.D.R. 21
- C-360/10 *SABAM v Netlog NV* [2012] 2 C.M.L.R. 18
- Joined Cases C-236/08 to C-238/08, *Google France Sarl v Louis Vuitton Malletier SA* [2010] E.T.M.R. 30
- C-145/10 *Painer v Standard Verlags GmbH* [2012] E.C.D.R. 6
- Joined Cases C-403/08 and C-429/08 *Football Association Premier League Ltd v QC Leisure* [2012] E.C.D.R. 8
- C-324/09 *L'Oréal SA v eBay International AG* [2011] E.T.M.R. 52
- C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH* [2009] ECR I-01227
- C-275/06 *Promusicae v Telefonica de Espana SAU* [2008] E.C.D.R. 10

NATIONAL COURTS

COUNTRY	CASE	TYPE
CYPRUS	23 April 2018 Court of Nicosia Ioannis Hatzioannou	Civil, Req. Info
CYPRUS	2 May 2018 Supreme Court of Cyprus Ioannis Chatzioannou and George Longkritis	Civil, Req. Info
CYPRUS	10 July 2018 Supreme Court of Cyprus Ioannis Hatzioannou and George Longkritis	Civil, Req. Info
CZECH REPUBLIC	27/2/2013 Supreme Court 8 Tdo 137/2013 'Liberec Pirate' CZ:NS:2013:8.TDO.137.2013.1	Criminal, hyperlinking
CZECH REPUBLIC	29/5/2013 Supreme Court 5 Tdo 271/2013 'ulozto.cz'	Criminal, hyperlinking
DENMARK	April 2015, Danish State Prosecutor for Serious Economic and International Crime (SØIK) Retten i Aalborg v. Private individual (Streaming site whargarbl.dk)	Criminal, hyperlinking
DENMARK	October 2015, Danish State Prosecutor for Serious Economic and International Crime (SØIK) Retten i Næstved v. Private individual (Streaming site floppi.org)	Criminal, hyperlinking
DENMARK	Københavns Byret (Copenhagen City Court) v Private individual Dec 2016	Criminal, STB
DENMARK	Østre Landsret 2011	Criminal, STB
FINLAND	Kopiosto v Telia Finland Oyj, Market Court, 18 June 2019, MAO:285/19	Civil, internet retransmission
FRANCE	9 octobre 2014 TGI Paris, 3rd Chamber, 1st section France Télévision v Playmedia; 2 February 2016 Appeal Court of Paris, pole 1 1st Chamber Playmedia v France Télévision	Civil, hyperlinking
FRANCE	18 juin 2010 TGI Paris M6 v SBDS	Civil, hyperlinking

FRANCE	19 Mars 2015 TGI Paris League de Football Professionnel v Puerto 80 (Rojadirecta)	Civil, hyperlinking
FRANCE	28/11/2013 Jugement au fond en la forme des référés (Article L. 336-2) Blocage et déréférencement : effet 12 mois	Civil, block/delist
FRANCE	04/12/2014 Jugement au fond en la forme des référés (Article L. 336-2 CPI) Blocage : effet 12 mois	Civil, block/de-list
FRANCE	02/04/2015 Jugement au fond en la forme des référés (Article L. 336-2 CPI) Blocage : effet 12 mois	Civil, block/de-list
FRANCE	07/07/2016 Jugement au fond en la forme des référés (Article L. 336-2 CPI) Blocage : effet 12 mois	Civil, block/de-list
FRANCE	06/07/2017 Jugement au fond en la forme des référés (Article L. 336-2) Blocage et déréférencement : effet 12 mois	Civil, block/de-list
FRANCE	02/11/2017 Jugement au fond en la forme des référés (Article L. 336-2 CPI) Blocage : effet 12 mois	Civil, block/de-list
FRANCE	15/12/2017 Jugement au fond en la forme des référés (Article L. 336-2 CPI) Blocage et déréférencement : effet 12 mois	Civil, block/de-list
FRANCE	25/05/2018 Jugement au fond en la forme des référés (Article L. 336-2 CPI) Blocage et déréférencement : effet 12 mois	Civil, block/de-list
FRANCE	14/12/2018 (RG 18/10652) Jugement au fond en la forme des référés (Article L. 336-2 CPI) Blocage et déréférencement : effet 12 mois	Civil, block/de-list
GERMANY	Regional Court Mannheim, 08 May 2015, 7 O 166/13	Civil, internet retransmission
GERMANY	Regional Court Mannheim, 08 May 2015, 7 O 166/13	Civil, internet retransmission
GERMANY	Regional Court of Munich I, 01 February 2018, 7 O 17752/17	Civil, block/de-list
GREECE	1909/2017 Athens Court of Appeal Operator of website www.livemovies.gr against AEPI	Civil, hyperlinking
GREECE	5249/2014 Multi-person Court of First Instance Operator of website www.livemovies.gr against AEPI (Greek collecting society for composers and lyricists)	Civil, hyperlinking
ITALY	17/08/2011 Tribunale Civile di Roma RTI c. Minan (Rojadirecta)	Civil, hyperlinking
ITALY	17/12/2011 Tribunale Civile di Roma RTI c. Minan (Rojadirecta)	Civil, hyperlinking
ITALY	Tribunale di Roma 26-10-2011 RTI v Worldstream	
ITALY	Tribunale di Roma 20-10-2012 RTI v Choopa	
ITALY	29/06/2013 Tribunale di Milano (Rojadirecta)	Civil, block/de-list
ITALY	24716, 15 Marzo 2016 Tribunale civile di Roma RTI c. TMFT Enterprises, LLC — Break Media	Civil, internet retransmission
ITALY	15 February 2019 Tribunale civile di Roma RTI c. Facebook	Civil, hyperlinking

NETHERLANDS	9 May 2018 C/03/233371 / HA ZA 17-158 ECLI:NL:RBLIM:2018:4395 District court Limburg — Stichting Brein v Leaper Beheer BV (also active as 'Flickstore', 'Dump Die Deal' and 'Live TV Store')	Civil, internet retransmission
NETHERLANDS	24 January 2018 C/09/485400 / HA ZA 15-367 ECLI:NL:RBDHA:2018:615 Court the Hague — The Football Association Premier League v Ecatel	Civil, internet retransmission
NETHERLANDS	27 October 2017 C/16/442373 / KG ZA 17-518 ECLI:NL:RBMNE:2017:5510 District court Midden-Nederland (summary proceedings) Stichting Brein v Moviestreamer International BV	Civil, hyperlinking
NETHERLANDS	17 October 2017 No 200.149.632/02 ECLI:NL:GHSHE:2017:4524 Court of Appeal's-Hertogenbosch MyP2P BV v The Football Association Premier League Limited BV e.a.	Civil, hyperlinking
NETHERLANDS	17 August 2016, C/09/515172 / KG ZA 16-905 ECLI:NL:RBDHA:2016:9685 Summary proceedings court the Hague N.V. Ado Den Haag et al. v Global Layer BV (04stream.com)	Civil, internet retransmission
NETHERLANDS	25 April 2017 C/01/320359/BP RK 17-324 Summary proceedings judge Court Oost-Brabant (<i>ex parte</i> proceedings) Initiated by Stichting Brein	Civil, hyperlinking
NETHERLANDS	2 December 2015C/16/400002 / KG ZA 15-675 ECLI:NL:RBMNE:2015:8685 District court Midden-Nederland (summary proceedings) Stichting Brein v [defendant]	Civil, STB
NETHERLANDS	10 June 2015 ECLI:NL:RBMNE:2015:4343 C/16/372666 / HL ZA 14-204 Court Midden-Nederland [asking preliminary questions, leading to HvJ EU 26 April 2017; C-527/15; ECLI:EU:C:2017:300] Stichting Brein v Filmspeler	Civil, STB
ROMANIA	Decision No 6422/19/10/2012 Supreme Court SRT acting as the claimant and CT acting as the defendant	Civil, internet retransmission
PORTUGAL	Court of Appeals of Évora 14 July 2010 case nr. 22/06.8FAVRS.E1 ZON TV Cabo Portugal SA v anonymised defendant	Civil, STB
SPAIN	Columbia Pictures et al v. Telefónica Espana et al 12 January 2017 Commercial Court No 6 of Barcelona	Civil, block/de-list
SWEDEN	NJA 2015 s. 1097 Supreme Court C More Entertainment AB, v Linus Sandberg	Civil, internet retransmission
UNITED KINGDOM	Twentieth Century Fox Film Corporation and Others v Sky UK Ltd and Others, [2015] EWHC (Ch.) 1082 ('Popcorn Time case') 28 April 2015	Civil, block/de-list
UNITED KINGDOM	Football Association Premier League Ltd v British Telecommunications Plc & Ors [2017] EWHC 480 (Ch.) (FAPL v BT I) 08 March 2017	Civil, block/de-list, STB

UNITED KINGDOM	Football Association Premier League Ltd v British Telecommunications Plc [2018] EWHC 1828 (Ch.) (FAPL v BT II) 18 July 2018	Civil, block/de-list, internet retransmission
UNITED KINGDOM	UEFA v BT [2018] EWHC 1900 (Ch.) 24 July 2018	Civil, block/de-list, internet retransmission
UNITED KINGDOM	Matchroom Boxing Ltd v BT Plc [2018] EWHC 2443 (Ch.) 20 September 2018	Civil, block/de-list, internet retransmission
UNITED KINGDOM	R v J.R., City of London Police, 9 December 2016 (unreported)	Criminal, STB
UNITED KINGDOM	R v W.O. and T.O., Nottingham Crown Court, 9 December 2016 (unreported)	Criminal, STB
UNITED KINGDOM	R v M.M. Teesside Crown Court, 6 March 2017 (unreported)	Criminal, STB
UNITED KINGDOM	R v B.T. and J.A., Teesside Crown Court, 20 October 2017 (unreported)	Criminal, STB
UNITED KINGDOM	R v S.K, P.R. and D.M., Warwick Crown Court, 19 February 2019 (unreported)	Criminal, STB

APPENDIX I — REVIEW OF POLICY, ECONOMIC AND TECHNICAL LITERATURE

Intellectual property right (IPR) infringement, particularly in the online environment, has not only been rising in volume but also in complexity. Much debate exists around the impact that IPR infringement may have on the creative industries and economy at large. Similarly, there is extensive literature on piracy online, as evidenced by references in a number of overview studies, including Danaher et al. (2013)⁽²³¹⁾ and Liebowitz (2013)⁽²³²⁾. This appendix reviews and summarises findings of prior research. The state of the art that is reviewed can be categorised accordingly:

- prior research estimating the magnitude of illegal IPTV in terms of active users;
- studies assessing the impact of IPTV and other media piracy on the sales and revenues of legal providers;
- studies estimating the revenue generated by unlawful IPTV providers.

The aim is to outline the most relevant findings with regard to IPTV online infringement and support the research of IPR-infringing business models, identification of challenges in tackling illegal IPTV, and quantitative analysis of illegal IPTV.

As reported by the EUIPO European Observatory on Infringements of Intellectual Property Rights (Observatory), IP rights help ensure that innovators and creators get a fair return for their work, encourage investment in research and create growth and quality jobs. The importance of IPR intensive industries is evidenced in the EUIPO Observatory study⁽²³³⁾ showing that IPR intensive industries generate 29.2 % jobs and contribute to 44.8 % of the GDP in European Union. The counterpart study conducted by the USPTO⁽²³⁴⁾ in 2012 reiterates the importance of IPR intensive industries reporting that nearly 35 % of the US GDP and 20 % of employment stems from the IP intensive sectors.

Nonetheless, multiple policy reports and economic studies confirm significant level of Intellectual Property (IP) infringement throughout the global markets and within the European Union. A recent EU level survey⁽²³⁵⁾ shows that on average 10 % of Europeans accessed or downloaded or streamed content from illegal online sources intentionally. This ratio varies across the Member States, reaching a high of 20 % in Slovenia, and a low of 5 % in Romania. Significant differences in online infringement rates suggest that piracy in the single market is not uniform. The reasons for this variation may stem from broadband penetration rates as well as distinct national demand and supply of illicit digital content.

⁽²³¹⁾ Danaher B., Smith M.D and R. Telang R 'Piracy and Copyright Enforcement Mechanisms', *Innovation Policy and the Economy*, Vol. 14, pp. 25-61, 2013.

⁽²³²⁾ Liebowitz S. 'The impact of internet piracy on sales and revenues of copyright owners', an abridged version of 'Internet piracy: the estimated impact on sales' in Handbook on the Digital Creative Economy Edited by Ruth Towse and Christian Handke, Edward Elgar, 2013, p. 35.

⁽²³³⁾ EPO and EUIPO: 'IPR-intensive industries and economic performance in the European Union', September 2019.

⁽²³⁴⁾ USPTO: 'Intellectual Property and the U.S. Economy: Industries in Focus', 2012.

⁽²³⁵⁾ EUIPO: 'European citizens and Intellectual Property. Perception, awareness and behaviour', March 2017.

Furthermore, piracy rates vary not only among countries but also among generations. The EUIPO ‘Intellectual Property and Youth’ scoreboard⁽²³⁶⁾ sets out the attitudes of 15-24 year olds toward IP. The survey shows that nearly one in four (21 %) young Europeans make intentional use of illegal sources when accessing digital content. It confirms the ever more acute problem among young consumers who represent a large market share for both legal and illegal IPTV services.

It is important to fully grasp the magnitude and trends of the illegal IPTV phenomenon in order to tackle it efficiently. Empirical studies and policy reports that analyse and provide empirical assessment of the illegal IPTV are also reviewed.

1.1 — MAGNITUDE OF ILLEGAL IPTV

Illegal IPTV seems to be a rapidly growing phenomenon throughout the global market. Much debate exists around the impact that online piracy has on creative sectors, and especially on the audiovisual industries. Given the relative novelty of internet television compared to cable and satellite technologies, most of earlier research and academic work studied the impact of piracy of physical movie copies, such as DVD or illegal movie downloads and peer-to-peer file sharing. Illegal IPTV presents quite a distinct case when estimating both its level and its impact. The shift in trend is also raised by the Hadopi ‘International Survey’ (2017)⁽²³⁷⁾ as they found that a large number of web users moved from peer-to-peer to streaming and more recently, toward illegal IPTV.

There are several studies that endeavour to estimate the level of illegal IPTV in terms of its users. Sandvine⁽²³⁸⁾ (2017) — the Canadian broadband management company — reports that 6.5 % of households in North America access known subscription television piracy services. According to their study ‘Subscription TV Piracy’, there are 7 million users of illicit TV content across the United States and Canada. As it is emphasised by the Kudelski Group⁽²³⁹⁾ (2016), piracy takes place in every country where people watch TV, however, the scale of piracy varies across the markets. In South America, for instance, a recent study found that an astonishing 50 %⁽²⁴⁰⁾ of internet users have accessed a site distributing pirated video content. Nearly 25 % of Australian internet users have streamed or downloaded content illegally, according to the Australian Department of Communications⁽²⁴¹⁾.

In Europe, a recent report by Nordic Content Protection (2017)⁽²⁴²⁾ estimates 400 000 illegal TV subscriptions across Sweden, Denmark, Norway and Finland. This represents 915 782 people aged 15–24, who deliberately download illegal content from the internet. The situation is not much better in

⁽²³⁶⁾ EUIPO: ‘Intellectual Property and Youth’ scoreboard, October 2019.

⁽²³⁷⁾ Hadopi: ‘International Survey: Key lessons learned from international benchmarking’, July 2017.

⁽²³⁸⁾ Sandvine: ‘2017 Global Internet Phenomena. Spotlight: Subscription TV Piracy’, 2017.

⁽²³⁹⁾ Kudelski Group: ‘The new face of pay-TV piracy and how to fight it’, 2016.

⁽²⁴⁰⁾ In Kudelski Group (2016), p. 2.

⁽²⁴¹⁾ In Kudelski Group (2016), p. 2.

⁽²⁴²⁾ Nordic Content Protection: ‘2017 Trend Report: Illegal distribution and sales of access to television broadcasts’, Oslo, Norway — January 2017.

the UK where recently commissioned research from the United Kingdom IP office (UKIPO, 2018) ⁽²⁴³⁾ estimates 15 % — or approximately 6.5 million UK internet users — consumed at least one item of online content illegally. 23 % of internet users illegally access TV programmes — this is the highest infringement level of any content type, relative to the 19 % online infringement of music and 13 % of books. Almost 9 % of British population admit to having illegally streamed at least one Premier League game over the past 12 months ⁽²⁴⁴⁾. Moreover, UKIPO ⁽²⁴⁵⁾ (2016/17) emphasised the importance of new technology such as set-top boxes, which makes streaming unlicensed TV programmes particularly effortless.

I.II — USE OF ILLICIT STREAMING DEVICES

Reports that estimate the number of Illicit Streaming Devices (ISDs), such as set-top boxes with pre-installed apps which enable consumers to access pirated IPTV content ⁽²⁴⁶⁾, find that this technology is ubiquitous in the current IPTV market. The ISDs, also just called ‘set-top-boxes’, ‘Kodi’, or ‘media players’, facilitate the streaming of copyright infringing IPTV content. This technology is abused by pirate sites and makes it possible to extract revenue charging consumers for the illicit IPTV subscriptions.

A recent consumer survey from YouGov (2017) ⁽²⁴⁷⁾ suggests that almost 5 million persons in the UK use pirated TV streaming services. It means that 10 % of the UK population has access to platforms such as pre-loaded streaming or boxes and sticks, and illegal streaming apps on smartphones and tablets, which allow accessing content from pirate sites. Furthermore, YouGov predicts that 2.6 million consumers expect to start accessing pirated streaming platforms in the future. According to Industry Trust for IP Awareness (2016) ⁽²⁴⁸⁾ even higher share of 19 % adults in the UK have used ISDs to access infringing content. As a point of reference, engagement with other, longer-standing forms of digital piracy via laptops and smartphones stands at 23 %.

Multiple studies draw attention to a rapid increase in the usage of ISDs. For instance, Industry Trust (2016) reveals an astonishing 143 % growth in associated Google searches in the UK during 2016 — a more advanced upward trajectory than for global searches. Hadopi’s (2017) International Survey ⁽²⁴⁹⁾ as well as the Office of the US Trade Representative (2017) ⁽²⁵⁰⁾ highlight the growing trend of illegal practices connected to media players, and focus on the threat that ISDs pose to content creators, sports leagues and live performances, as well as legitimate streaming, on-demand and over-the-top

⁽²⁴³⁾ UK IPO and Kantar Media: ‘Online Copyright Infringement Tracker: Overview and key findings’, March 2018.

⁽²⁴⁴⁾ Research from personal finance comparison site finder.com: <https://advanced-television.com/2019/10/11/9-brits-admit-illegally-streaming-premier-league-in-last-year>.

⁽²⁴⁵⁾ UK IPO: ‘IP Crime and Enforcement Report’, 2016/2017.

⁽²⁴⁶⁾ So-called ‘fully-loaded’ set-top boxes.

⁽²⁴⁷⁾ <https://yougov.co.uk/news/2017/04/20/almost-five-million-britons-use-illegal-tv-streami/>

⁽²⁴⁸⁾ The Industry Trust: ‘IPTV Piracy: A study on set-top-box and stick infringement for the industry’, 2016.

⁽²⁴⁹⁾ Hadopi: ‘International Survey: Key lessons learned from international benchmarking’, July 2017.

⁽²⁵⁰⁾ Office of the US Trade Representative: ‘2017 Out-of-Cycle Review of Notorious Markets’, 2017.

media service providers. According to the IDATE study conducted for Hadopi in 2017, there were 2.4 million ISD users in France, out of which 1.5 million users had access to pirated TV content. This represented 3.8 % of internet users. Hadopi also estimates there are 91 000 content-infringing boxes that are currently active. In the North America region, Sandvine (2017) ⁽²⁵¹⁾ concludes that 68.6 % of the 8.8 % of households with 'Kodi', or roughly 6 % of all households, currently have a 'Kodi' device configured to access unlicensed content. Globally, the Motion Picture Association of America (MPAA, 2017) ⁽²⁵²⁾ suggests that of 38 million users of 'Kodi' set-top-box software, there are 26 million (68.5 %) users who have add-ons that enable them to access pirated IPTV content.

I.III — IMPACT OF ILLEGAL IPTV

It is clear that a not unsubstantial share of the population across global markets is engaged in pirated IPTV service consumption. Even though there is no comprehensive prognosis on piracy levels, the technological developments suggest that demand for easily accessible TV and video-on-demand content online will gain momentum in upcoming years. The prospect of millions of people choosing to watch films and TV content illegally through a simple set-top device could have far-reaching consequences for the audiovisual industry and the wider economy.

The above reviewed studies estimate the number of consumers who are using pirated IPTV services. The effect that the magnitude of illegal IPTV has on legal content providers and legitimate IPTV market revenue is a different question. As noted by Danaher et al. (2013) 'one cannot analyse how governments and industries should respond to piracy without first analysing whether there is a need to respond.'

Most academic studies support the assumption that media piracy harms sales as concluded by Smith and Telang ⁽²⁵³⁾ (2012) and Danaher, Smith and Telang ⁽²⁵⁴⁾ (2013). In 2015 ⁽²⁵⁵⁾ the same authors found that out of 21 papers that examined the link between piracy and sales, 18 found a negative impact and only three found none. Liebowitz ⁽²⁵⁶⁾ (2013) arrives at a similar result. Out of the seven articles identified on the impact of piracy on box office revenues or video sales/rentals, all find piracy to be harmful. His analysis leads him to conclude that the harm from piracy to the movie industry is large.

⁽²⁵¹⁾ Sandvine: '2017 Global Internet Phenomena. Spotlight: the "fully loaded" Kodi ecosystem', 2017.

⁽²⁵²⁾ Motion Picture Association of America: 'Public comment on the 2017 Special 301 Out of Cycle Review of Notorious Markets. Docket No USTR-2017-0015', 2 October 2017.

⁽²⁵³⁾ Smith M. D. and R. Telang: 'Assessing the Academic Literature Regarding the Impact of Media Piracy on Sales', 2012

⁽²⁵⁴⁾ Danaher B., M. D. Smith and R. Telang: 'Piracy and Copyright Enforcement Mechanisms', *Innovation Policy and the Economy*, Vol. 14, pp. 25-61, 2013.

⁽²⁵⁵⁾ Danaher B., M. D. Smith and R. Telang: 'Copyright Enforcement in the Digital Age: Empirical Economic Evidence and Conclusions', Advisory Committee on Enforcement, Tenth Session, Geneva, November 23 to 25, 2015, World Intellectual Property Organization.

⁽²⁵⁶⁾ Liebowitz S.: 'The impact of internet piracy on sales and revenues of copyright owners', an abridged version of 'Internet piracy: the estimated impact on sales' in *Handbook on the Digital Creative Economy*, Edited by Ruth Towse and Christian Handke, Edward Elgar, 2013, p. 35.

One of the most comprehensive studies that measure the impact of online piracy is commissioned by the European Commission. The study⁽²⁵⁷⁾ on the relation between online copyright infringement (digital piracy) and sales of copyrighted content adds to the existing literature assessing displacement rates in the presence of an important recent phenomenon, i.e. the widespread availability of a wide variety of services for downloading or streaming content. In general, the results do not show robust statistical evidence of displacement of sales by online copyright infringements. That does not necessarily mean that piracy has no effect but only that the statistical analysis does not prove with sufficient reliability that there is an effect. An exception is the displacement of recent top films. The results show a displacement rate of 40 % which means that for every 10 recent top films watched illegally, four fewer films are consumed legally.

Only a few economic studies focus on assessing potential losses that illegal IPTV causes to legitimate service providers. YouGov (2017), for example, suggests that one in seven consumers accessing infringing content cancelled at least one legitimate paid-for TV service within a year since starting to access pirated IPTV. In addition, nearly a third (31 %) of those who use pirated streaming platforms but who have paid-for TV services believe they will cancel their subscriptions over the next 12 months. Industry Trust⁽²⁵⁸⁾ research states the direct impact that illegal IPTV has on consumer spending. The survey shows that two in five (41 %) of those engaging in illegal IPTV claim to spend less money on going to the cinema, compared to 22 % who engage in other forms of piracy. Set-top box infringers are also 15 % more likely to spend less money on paid-subscription services like Sky, Virgin TV and Now TV.

Technological challenges must too be taken into account when considering the impact of illegal IPTV. Such technological developments as the spread of broadband penetration and higher internet speed do not only facilitate access to legitimate IPTV sources, but indeed simplifies access to those that are illicit. The Nordic Content Protection (2017) Trend Report confirms the rapid increase of illegal IPTV distributors, with the main sales taking place on dedicated websites on the open internet. Their figures show that piracy costs the Swedish film and TV industries EUR 330 million annually, which equates to a quarter of the industry's total revenue. Illegal distribution networks in the Nordic region (Sweden, Norway, Denmark and Finland) represent a lost earning potential of approximately EUR 531.6 million to legal distributors. Sandvine (2017) report estimates that illegal IPTV generates losses to the entertainment industry of roughly USD 4.2 billion a year in North America.

I.IV — REVENUE SOURCES

Nordic Content Protection (2017) describes IPTV piracy as 'highly lucrative, white-collar crime'. As a considerable share of consumers chooses to stream TV content illegally, it reasonable to expect that this content is made available by pirate sites in order to make profits.

⁽²⁵⁷⁾ European Commission: 'Estimating displacement rates of copyrighted content in the EU', May 2015.

⁽²⁵⁸⁾ The Industry Trust: 'IPTV Piracy: A study on set-top-box and stick infringement for the industry', 2016.

In general, there are three revenue sources for illegal IPTV providers: subscription, advertising and malware. As reported by UKIPO⁽²⁵⁹⁾, subscriptions are one of the main ways that illicit IPTV and illicit streaming device providers make their money, charging monthly fees to give access to paid-for channels. Nordic Content Protection (2017) confirms that illegal networks are managed similarly to legitimate business: they have a clear structure, with designated personnel in charge of sales, finance and technology. Some of the larger criminal networks operate behind a legitimate façade, quite often a retail store selling decoding devices, and other related merchandise, making substantial illegal revenue. Advertising presents another major source of income for pirate sites. The Digital Citizens Alliance (2014) study⁽²⁶⁰⁾ in the US of almost 600 ‘content theft’ websites (featuring illegal streams or downloads) found that they earned an estimated USD 227 million in annual advertising revenue. Another recent Digital Citizens Alliance (2017) report⁽²⁶¹⁾ found that one in every three visitors of content theft sites are exposed to malware. The study found that the organised groups behind content theft websites are making at least USD 70 million a year by charging hackers to put malware on their sites that will then infect visitors’ computers.

Sandvine (2017) reports that the TV piracy ecosystem, including unlawful device sellers and unlicensed video providers and video hosts, stands to bring in revenue of an estimated USD 840 million a year in North America alone. Nordic Content Protection (2017) estimates a yearly turnover of approximately EUR 80 million for the distributors of illegal content in Sweden, Norway, Denmark and Finland. Hadopi (2017) reports that the market of unlawful boxes represented EUR 2.43 million in France: EUR 1.14 million generated from the sale of boxes, EUR 1.11 million stem from the sale of subscriptions to illegal IPTV services via ‘Kodi’, and EUR 180 000 from advertising revenue. If the current trend is confirmed, Hadopi expects the illegal earnings will rise to EUR 3.28 million by 2020. A recent report commissioned by BASCAP and INTA (2017)⁽²⁶²⁾ sets the value of digitally pirated movies at about USD 160 billion. These studies by Sandvine (2017), Nordic Content Protection (2017) and BASCAP and INTA (2017) base their findings on the ‘bottom-up’ methodology. It starts from a measure of the volume of illegal IPTV expressed in number of users, subscriptions or illicit movie downloads. This volume measure is then matched with data on IPTV subscription charged by illegal providers. In the case of the BASCAP and INTA (2017) report, the value of the pirated movie is in line with the prices charged by legal content providers — specifically prices associated with the activities for which pirated films are substitutes.

Overall, the existing economic research indicates that unauthorised IPTV services have a substantial and growing base of users and is ever present throughout the global markets. The empirical evidence confirms that copyright infringing IPTV content providers generate considerable revenue from these activities.

⁽²⁵⁹⁾ UK IPO: ‘Cracking down on Digital Piracy Report’, September 2017.

⁽²⁶⁰⁾ Digital Citizens Alliance: ‘Good Money Gone Bad. Digital Thieves and the Hijacking of the Online Ad Business. A Report on the Profitability of Ad-Supported Content Theft’, February 2014.

⁽²⁶¹⁾ Digital Citizens Alliance: ‘Trouble in Our Digital Midst: How Digital Platforms Are Being Overrun by Bad Actors and How the Internet Community Can Beat Them at Their Own Game’, June 2017.

⁽²⁶²⁾ Frontier Economics: ‘The economic impacts of counterfeiting and piracy. Report prepared for BASCAP and INTA’, 2017.

I.V — TECHNICAL LITERATURE ON ILLEGAL IPTV

The methodology for the technical aspects of the project considered the scientific literature as well as technical reports in the domain of audiovisual streaming technologies and enablers for illicit streaming. The particular literature themes were selected in order to develop an understanding of the technologies, identify the actors involved in the illegal streaming and present the communication structures and dynamics of these actors.

During the first phase of the research, the terminology and different content transmission technologies were set. Appendix III shows the diagram produced which is a tessellation of the different technologies.

The work by Rafique et al. (2016)⁽²⁶³⁾ explores the free live-streaming services and provides the motivation of offering ‘free’ streaming to users. The technical instruments for this work were screen scraping through web browser automation tools, keyword searching and classification of the pages through data mining software (weka). It was evident that the availability of free services is popular as it has a relatively substantial customer base; as it is ‘free’, the expectations of quality of service and customer support are limited but at the same time the revenue streams seem significant, as they capitalise upon advertising and malware delivery. Indicatively, over 5 000 streaming domains were identified and the main actors were aggregators, illegal content providers and advertisers.

Ibosiola et al. (2018)⁽²⁶⁴⁾ focused particularly on aggregators (which are referred to as *indexing sites* by these researchers) and cyberlockers. They studied the extent of these services through network analysis (based on domains and Autonomous Systems) as well as similarities of the underlying HTML⁽²⁶⁵⁾ pages. Although there are several aggregators and cyberlockers available, it was realised that this is a remarkably centralised system with just a few networks, countries and cyberlockers underpinning most provisioning. The researchers identified 1 903 distinct hosts providing streaming content and have also studied the number of takedown requests. From this research the actors identified and verified were the video uploader, streaming cyberlocker and indexing party (aggregator) but also an important finding was the hosting provider and their role, who, despite being considered the ‘neutral’ party in the sense that they mainly act as a facilitator and enabler of internetworking and web services in general, the fact that there are some hosting providers who are more preferred than others in illegal streaming, causes interesting further questions that deserve to be explored.

⁽²⁶³⁾ Rafique M. Z., Van Goethem T., Joosen W., Huygens C., and Nikiforakis N.: ‘It’s Free for a Reason: Exploring the Ecosystem of Free Live Streaming Services’, 2016.

⁽²⁶⁴⁾ Ibosiola D., Steery B., Garcia-Recueroy A., Stringhiniz G., Uhligy S., and Tysony G.: ‘Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers’, 2018.

⁽²⁶⁵⁾ HTML (Hypertext Markup Language) — a standardised system for tagging text files to achieve font, colour, graphic, and hyperlink effects on world wide web pages.

APPENDIX II — CASE STUDIES OF INTELLECTUAL PROPERTY RIGHTS' INFRINGING ONLINE BUSINESS MODELS APPLIED BY UNAUTHORISED IPTV PROVIDERS

Case studies of Intellectual Property Rights' infringing business models in the IPTV market are identified and analysed in this section. The selected case studies are defined according to the methodology developed in 'Research on Online Business Models Infringing Intellectual Property Rights', Phase 1 — Establishing an overview of online business models infringing intellectual property rights.

The case studies are representative to business models adapted by providers of unlawful IPTV, as summarised in the section 2 in this report.

Case studies are analysed within the framework of three main business models adapted by illegal IPTV providers:

II.I — ILLEGAL IPTV SUBSCRIPTION ONLINE BUSINESS MODEL ('IPTV RETAILERS')

IPTV resellers are websites that offer access to numerous live TV channels for a subscription price. The wide selection of channels are from European, US, Arabic, Russian, Asian and other countries. The service can be used on a TV set, most commonly enabled via a set-top-box, on PCs, smartphones and tablets.

Most websites present a user-friendly interface and a modern layout, which makes it easy to subscribe and make a payment. In order to access the service, users usually have to pay a monthly fee. An attractive feature is that there is no binding contract period (which means that the subscriber can quit the service at any time) and the process of registration is very simple. Payments are usually made through PayPal accounts or credit/debit cards, but some services accept also payment by cryptocurrencies (Bitcoin).

Websites vary in their social media presence, with some websites that have Facebook or Twitter accounts. Most of the websites have a customer support function and contacts can be made through email or live-chat. Due to their overall design, user interface and customer support, these websites may trick the layperson into believing that they offer a legal service.

Websites are categorised as a non-deceptive business model. Revenues are made from subscription payments.

II-II — ILLEGAL IPTV FOR RESELLERS ('IPTV WHOLESALERS')

The websites sell access to servers and a streaming possibility of the packages of numerous live TV channels. Payments are charged as a monthly subscription. The customers can further sell the IPTV streaming service to multiple individuals. For this reason, this is identified as a business-to-business (b2b) model.

In order to access the service, users must register and purchase a certain amount of 'credits' in order to be able to start accessing the live channel streams. Normally, one credit equals to one euro. Payments are made through PayPal accounts or credit/debit cards. Payments in Bitcoin is encouraged through a discount.

Explicit tutorials are provided that explain how to set up a website to offer IPTV services, to manage customers and payments. The website interface is simple and user-friendly.

The websites are categorised as a non-deceptive business model. Revenues are made from reseller-subscription payments.

II-III — ILLEGAL IPTV FREE STREAMING PORTALS ('LINK AGGREGATORS')

Websites on the open internet are facilitating access to copyright-protected TV channel broadcasts. The users of the website can browse or search through the website to find links that would allow them access to the live broadcasts. The links would lead to a different file sharing networks through which content could be downloaded.

The website links section appeared to be maintained thoroughly and each link verified. Many operators have social media presence and an online customer support function. Usually simple and explicit tutorials on free IPTV streaming (e.g. m3u file download or set-top box install) are made available on these websites.

It has not been analysed whether the shared content or the advertising on the website has malware. Therefore, it cannot be determined whether the business model is deceptive or not.

Illegal IPTV Subscription

Case study number 1: Suspected unauthorised IPTV subscription selling website

Date of analysis: 01/03/2019 - 21/06/2019

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Unauthorised IPTV subscription vendors offer access to numerous multinational TV channels. Usually they provide high quality streaming.

Websites may vary in their social-media presence, pricing strategies and IPTV content provided. Some vendors include access to vast video on demand libraries (movies, TV series). Most websites present a user-friendly interface and are simple to use.

To access the service, customers have to pay a monthly subscription fee. Subscription period normally is for 1, 3 or 6 months. An attractive feature is that there is no binding contract period. Payments can be made with credit or debit cards, or through PayPal accounts. Some vendors also accept payments with crypto currencies (e.g. Bitcoin). Most websites have a customer support function and queries can be made through email or live-chat. Due to their overall design, user interface and customer support, these websites may be easily confused with a legitimate service. Websites are categorised as a non-deceptive business model. Revenues are made from direct sales of subscriptions.

Matrix

Online Digital Platform

A

Internet Site
Controlled by
Infringer

B

Third Party
Marketplace

C

Social Media or
Blog

D

Gaming or
Virtual World

E

E-mail,
Chatroom or
Newsgroup

F

Mobile Devices

1 Domain Name or Digital Identifier Misuse of IPR

A1

B1

C1

D1

E1

F1

2 Physical or Virtual Product Marketing

A2

B2

C2

D2

E2

F2

3 Digital Content Sharing

A3

B3

C3

D3

E3

F3

4 Account Access or Codes to Digital Content Sharing

A4

B4

C4

D4

E4

F4

5 Phishing, Malware Dissemination or Fraud

A5

B5

C5

D5

E5

F5

6 Contributing to Infringement

A6

B6

C6

D6

E6

F6

Digital Platform & Technology:

Open internet.
IPTV services are accessible to registered users for a fee.

Products and Services:

Website offers streaming access to more than 3 000 TV channels. Average price is EUR 13 a month. Customers can stream IPTV on multiple devices including smartphones and tablets. In addition, this vendor offers IPTV to resellers, though it is not advertised in an obvious manner and information is only available upon email request.

Involved IPR(s):

Copyright and related rights
Trade marks

Identification of Infringer:

The server location is in Europe, as specified by the suspected infringer on its website. Registrant name is associated with another suspected-infringing website for cardsharing and IPTV server subscription. Registrant country is identified in Afghanistan through domain name registry WHOIS information.

Revenue Sources:

Revenue is made from direct sales of unauthorised IPTV subscriptions. Payments are made with credit cards and via PayPal.

Customer Relations:

The service has no binding period. Instant delivery is upon subscription payment. Websites do not describe any usage restrictions or limitations. Based on this, it appears the service is available worldwide. The website has customer support messaging function via email and guarantees a 24-hour response. Website also has a newsletter option conditional upon subscription.

Resilience Against Enforcement Action:

The website has changed various top-level domains after being de-indexed by Google further to a DMCA request submitted by Sky Italia Srl in May 2019.

Marketing Channels and Internet Traffic Features:

An Android app for services is made available at APKPure website. The website does not have social media accounts. The user base appears to be collected by a mouth-to-mouth marketing strategy. The website also has a newsletter that is sent out to registered email addresses.

Users are well informed on the website services. However, the risk for abuse of the website users' personal or payment data remains.

Customer Incentives:

Pricing strategy encourages longer binding subscription period, e.g. annual subscription costs EUR 8 a month, while a single month price is EUR 20.

Illegal IPTV Subscription

Case study number 2: Suspected unauthorised IPTV subscription selling website

Date of analysis: 01/03/2019 - 21/06/2019

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Unauthorised IPTV subscription vendors offer access to numerous multinational TV channels. Usually they provide high quality streaming. Websites may vary in their social-media presence, pricing strategies and IPTV content provided. Some vendors include access to vast video on demand libraries (movies, TV series). Most websites present a user-friendly interface and are simple to use.

To access the service, customers have to pay a monthly subscription fee. Subscription period normally is for 1, 3, 6, or 12 months. An attractive feature is that there is no binding contract period. Payments can be made with credit or debit cards, or through PayPal accounts. Some vendors also accept payments with crypto currencies (e.g. Bitcoin). Most websites have a customer support function

and queries can be made through email or live-chat. Due to their overall design, user interface and customer support, these websites may be easily confused with a legitimate service. Websites are categorised as a non-deceptive business model. Revenues are made from direct sales of subscriptions.

Matrix

Online Digital Platform

IPR Infringing Activity

A

Internet Site Controlled by Infringer

B

Third Party Marketplace

C

Social Media or Blog

D

Gaming or Virtual World

E

E-mail, Chatroom or Newsgroup

F

Mobile Devices

1 Domain Name or Digital Identifier Misuse of IPR

A1

B1

C1

D1

E1

F1

2 Physical or Virtual Product Marketing

A2

B2

C2

D2

E2

F2

3 Digital Content Sharing

A3

B3

C3

D3

E3

F3

4 Account Access or Codes to Digital Content Sharing

A4

B4

C4

D4

E4

F4

5 Phishing, Malware Dissemination or Fraud

A5

B5

C5

D5

E5

F5

6 Contributing to Infringement

A6

B6

C6

D6

E6

F6

Digital Platform & Technology:

Open internet. IPTV services are accessible to registered users for a fee. There is an option to access selected IPTV services for free as well.

Products and Services:

Website offers streaming access to more than 6 500 TV channels and an unidentified number of VoDs. Indicated price is EUR 27.60 for 3 months. Customers can stream IPTV on multiple devices including smart TVs, smartphones and tablets. Moreover, registered users have option to stream a few preselected TV channels for free.

Involved IPR(s):

Copyright and related rights
Trade marks

Identification of Infringer:

IP address location is identified in Germany. Registrant Information is redacted for privacy except for the country (Germany) and the email address. Website owner information is protected by a third-party company which registered the DNS.

Revenue Sources:

Revenue is made from direct sales of unauthorised IPTV subscriptions. Payments are accepted with Visa, MasterCard, American Express and Discovery.

Customer Relations:

The service has no binding period. Instant delivery is upon subscription payment. Websites do not describe any usage restrictions or limitations. Based on this, it appears the service is available worldwide. The website has a live-chat function and customer support messaging function via email. The website also has a FAQ section.

Resilience Against Enforcement Action:

N/A

Users are well informed on the website services. However, the risk for abuse of the website users' personal or payment data remains.

Marketing Channels and Internet Traffic Features:

The website has a supporting blog. Channels can be streamed on Android TV, set-top boxes, tablets and smartphones. A viewing application can be downloaded from the Google Play store or directly as an APK (Android package) from the website. There are no social media accounts.

Customer Incentives:

Customers are drawn in by the free preselected channel offer. In addition, the website offers a free 24-hour trial of the full IPTV service.

Illegal IPTV Subscription

Case study number 3: Suspected unauthorised IPTV subscription selling website

Date of analysis: 01/03/2019 - 21/06/2019

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Unauthorised IPTV subscription vendors offer access to numerous multinational TV channels. Usually they provide high quality streaming. Websites may vary in their social-media presence, pricing strategies and IPTV content provided. Some vendors include access to vast video on demand libraries (movies, TV series). Most websites present a user-friendly interface and are simple to use.

To access the service, customers have to pay a monthly subscription fee. Subscription period normally is for 1, 3, 6, or 12 months. An attractive feature is that there is no binding contract period. Payments can be made with credit or debit cards, or through PayPal accounts. Some vendors also accept payments with crypto currencies (e.g. Bitcoin). Most websites have a customer support function

and queries can be made through email or live-chat. Due to their overall design, user interface and customer support, these websites may be easily confused with a legitimate service. Websites are categorised as a non-deceptive business model. Revenues are made from direct sales of subscriptions.

Matrix

Online Digital Platform

IPR Infringing Activity

A

Internet Site Controlled by Infringer

B

Third Party Marketplace

C

Social Media or Blog

D

Gaming or Virtual World

E

E-mail, Chatroom or Newsgroup

F

Mobile Devices

1 Domain Name or Digital Identifier Misuse of IPR

A1

B1

C1

D1

E1

F1

2 Physical or Virtual Product Marketing

A2

B2

C2

D2

E2

F2

3 Digital Content Sharing

A3

B3

C3

D3

E3

F3

4 Account Access or Codes to Digital Content Sharing

A4

B4

C4

D4

E4

F4

5 Phishing, Malware Dissemination or Fraud

A5

B5

C5

D5

E5

F5

6 Contributing to Infringement

A6

B6

C6

D6

E6

F6

Digital Platform & Technology:

Open internet. IPTV services are accessible to registered users for a fee.

Products and Services:

Website offers streaming access to more than 12 000 TV channels and over 3 000 VoDs. Indicated price is EUR 25 for 3 months, EUR 45 for 6 months, and EUR 75 for a 12-month period. In addition, IPTV packages are offered for re-sellers.

Involved IPR(s):

Copyright and related rights
Trade marks

Identification of Infringer:

The IP address location is identified in Germany. Contact details provided on the website are associated with a location in Denver, USA. Website owner information is protected by a third-party company which registered the DNS.

Revenue Sources:

Revenue is made from direct sales of unauthorised IPTV subscriptions. Payments are made through a billing platform. The vendor accepts Bitcoin, or payments via PayPal.

Customer Relations:

The paid service has a binding period from 3-12 months, depending on the length of subscription. Instant delivery is upon subscription payment. The website does not describe any usage restrictions or limitations. Based on this, it appears the service is available worldwide. A customer support function is available via email or phone. The website also has a tutorial section facilitating installation and first-time use.

Resilience Against Enforcement Action:

The website has been identified as an infringer and de-indexed by Google further to two DMCA complaints submitted in March and April 2019. The website operates under different top-level domains and aliases.

Marketing Channels and Internet Traffic Features:

The website has WhatsApp and Facebook accounts that increase its online exposure and allows it to reach out to a broader audience. Customers can stream the channels on multiple devices, including smart TVs, smartphones and tablets.

Users are well informed on the website services. However, the risk for abuse of the website users' personal or payment data remains.

Customer Incentives:

The vendor has a pricing strategy encouraging longer binding subscription periods by reducing the monthly price. A free 24-hour trial is offered.

Illegal IPTV Subscription

Case study number 4: Suspected unauthorised IPTV subscription selling website

Date of analysis: 01/03/2019 - 21/06/2019

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Unauthorised IPTV subscription vendors offer access to numerous multinational TV channels. Usually they provide high quality streaming. Websites may vary in their social-media presence, pricing strategies and IPTV content provided. Some vendors include access to vast video on demand libraries (movies, TV series). Most websites present a user-friendly interface and are simple to use.

To access the service, customers have to pay a monthly subscription fee. Subscription period normally is for 1, 3, 6, or 12 months. An attractive feature is that there is no binding contract period. Payments can be made with credit or debit cards, or through PayPal accounts. Some vendors also accept payments with crypto currencies (e.g. Bitcoin). Most websites have a customer support function and queries can be made through email or live-chat. Due to their overall design, user interface and customer support, these websites may be easily confused with a legitimate service. Websites are categorised as a non-deceptive business model. Revenues are made from direct sales of subscriptions.

Matrix

Online Digital Platform

A

Internet Site Controlled by Infringer

B

Third Party Marketplace

C

Social Media or Blog

D

Gaming or Virtual World

E

E-mail, Chatroom or Newsgroup

F

Mobile Devices

1 Domain Name or Digital Identifier Misuse of IPR

A1

B1

C1

D1

E1

F1

2 Physical or Virtual Product Marketing

A2

B2

C2

D2

E2

F2

3 Digital Content Sharing

A3

B3

C3

D3

E3

F3

4 Account Access or Codes to Digital Content Sharing

A4

B4

C4

D4

E4

F4

5 Phishing, Malware Dissemination or Fraud

A5

B5

C5

D5

E5

F5

6 Contributing to Infringement

A6

B6

C6

D6

E6

F6

Digital Platform & Technology:

Open internet. IPTV services are accessible to registered users for a fee.

Products and Services:

Website offers streaming access to nearly 260 TV channels complemented with VoD library. Average monthly subscription price is EUR 22. Clients can purchase a subscription with the set-top box hardware included. Also, Double Play (IPTV & VOIP) packages and an App is available on Google play & App Store.

Involved IPR(s):

Copyright and related rights

Identification of Infringer:

The IP address location is identified in the United States of America. Website owner information is protected by a third-party company which registered the DNS. The registrant country is identified as USA in the domain name registry WHOIS information.

Revenue Sources:

Revenue is generated from direct sales of suspected unauthorised IPTV subscriptions. Payments with credit and debit cards, such as Visa, MasterCard, Discover and American Express are accepted.

Customer Relations:

The service has no binding period. Instant delivery is upon subscription payment. The website does not describe any usage restrictions or limitations. Based on this, it appears the service is available worldwide. Hardware delivery is restricted to U.S. customers. The vendor has a helpdesk function and a messaging queries form. Continuous 24/7 hours support is ensured. Customers can also contact the vendor by phone, email or visit their office in the U.S. Users are well informed on the website services. However, the risk for abuse of the website users' personal or payment data remains.

Resilience Against Enforcement Action:

IPTV subscriptions offered by this vendor are suspected to be unauthorised. However, some of the channels are possibly provided legitimately, as the site provides information claiming it has obtained direct licenses from Bangladeshi TV channels to offer their content globally.

Marketing Channels and Internet Traffic Features:

The website has Twitter and YouTube social accounts that help in expanding its audience reach out.

Customer Incentives:

Vendor has a pricing strategy encouraging longer binding subscription periods by reducing the monthly price. A free 14-day trial is offered.

Illegal IPTV Subscription

Case study number 5: Suspected unauthorised IPTV subscription selling website

Date of analysis: 01/03/2019 - 21/06/2019

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Unauthorised IPTV subscription vendors offer access to numerous multinational TV channels. Usually they provide high quality streaming. Websites may vary in their social-media presence, pricing strategies and IPTV content provided. Some vendors include access to vast video on demand libraries (movies, TV series). Most websites present a user-friendly interface and are simple to use. To access the service, customers have to pay a monthly subscription fee. Subscription period normally is for 1, 3, 6, or 12 months. An attractive feature is that there is no binding contract period. Payments can be made with credit or debit cards, or through PayPal accounts. Some vendors also accept payments with crypto currencies (e.g. Bitcoin). Most websites have a customer support function and queries can be made through email or live-chat. Due to their overall design, user interface and customer support, these websites may be easily confused with a legitimate service. Websites are categorised as a non-deceptive business model. Revenues are made from direct sales of subscriptions.

Matrix	Online Digital Platform	A	B	C	D	E	F
		Internet Site Controlled by Infringer	Third Party Marketplace	Social Media or Blog	Gaming or Virtual World	E-mail, Chatroom or Newsgroup	Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology:

Open internet. IPTV services are accessible to registered users for a fee.

Products and Services:

Website offers streaming access to 4 000 TV channels complemented with VoD library. The website is in French. The average monthly subscription price is EUR 10.62. A reseller panel option is also offered in this case.

Involved IPR(s):

Copyright and related rights

Identification of Infringer:

The server location is identified in Germany. Registrant information is redacted for privacy. The website owner information is protected by a third-party company which registered the DNS.

Revenue Sources:

Revenue is generated from direct sales of suspected unauthorised IPTV subscriptions. Payments are made with credit and debit cards. Additionally, payments can be made via PayPal or with Bitcoin.

Customer Relations:

The service has no binding period. Instant delivery is upon subscription payment. The website does not describe any usage restrictions or limitations. Based on this, it appears the service is available worldwide. The vendor has a customer support contact form and online chat function. Continuous 24/7 support is ensured. Customers can also contact the vendor by email.

Resilience Against Enforcement Action:

The service has not been subject to blocking or de-indexing actions.

Marketing Channels and Internet Traffic Features:

The website has Twitter, Pinterest, Instagram and YouTube social accounts. Customers can stream IPTV on multiple devices, including smartphones, tablets, smart TVs, or PCs. The vendor indicates that software such as Android, iOS, Mac and Windows is supported.

Users are well informed on the website services. However, the risk for abuse of the website users' personal or payment data remains.

Customer Incentives:

The vendor has a pricing strategy encouraging longer binding subscription periods by reducing the monthly price. A free 48-hour trial is offered.

Illegal IPTV Subscription

Case study number 6: Suspected unauthorised IPTV subscription selling website

Date of analysis: 01/03/2019 - 21/06/2019

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Unauthorised IPTV subscription vendors offer access to numerous multinational TV channels. Usually they provide high quality streaming. Websites may vary in their social-media presence, pricing strategies and IPTV content provided. Some vendors include access to vast video on demand libraries (movies, TV series). Most websites present a user-friendly interface and are simple to use.

To access the service, customers have to pay a monthly subscription fee. Subscription period normally is for 1, 3, 6, or 12 months. An attractive feature is that there is no binding contract period. Payments can be made with credit or debit cards, or through PayPal accounts. Some vendors also accept payments with crypto currencies (e.g. Bitcoin). Most websites have a customer support function and queries can be made through email or live-chat. Due to their overall design, user interface and customer support, these websites may be easily confused with a legitimate service. Websites are categorised as a non-deceptive business model. Revenues are made from direct sales of subscriptions.

Matrix	Online Digital Platform	A	B	C	D	E	F
		Internet Site Controlled by Infringer	Third Party Marketplace	Social Media or Blog	Gaming or Virtual World	E-mail, Chatroom or Newsgroup	Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology:

Open internet. IPTV services are accessible to registered users for a fee.

Products and Services:

Website offers streaming access to over 7 000 TV channels (200 sports channels) complemented with a multi-language VoD library. The monthly subscription price starts at EUR 9.99. The website is in English language

Involved IPR(s):

Copyright and related rights

Identification of Infringer:

Registrant information is redacted for privacy. IP address location is identified in the USA. Exact server location could not be identified as the site uses 'Cloudflare' hosting to hide its real IP address. More in-depth investigation locates the server and IP address in Malta. The website owner information is protected by a third-party company which registered the DNS.

Revenue Sources:

Revenue is generated from direct sales of suspected unauthorised IPTV subscriptions. Payment methods are via PayPal, Skrill, and Bitcoin. The vendor applies a filter to recognise temporary email addresses upon payment delivery, thus protecting itself from unwanted investigations or reducing the risk of non-payments.

Customer Relations:

The service has no binding period. Instant delivery is upon subscription payment. The website does not describe any usage restrictions or limitations. Based on this, it appears the service is available worldwide.

Resilience Against Enforcement Action:

The domain name 'x.com' was de-indexed by Google in March 2019. The service now operates under the TLD '.co' and features prominently in Google's search results.

The vendor has a customer online support contact form. There are no other contact details indicated though. Moreover, website has an FAQ section.

Marketing Channels and Internet Traffic Features:

The website has Twitter social accounts that assists in expanding its audience outreach. Customers can stream IPTV on multiple devices, including smartphones, tablets, smart TVs, or PCs.

Users are well informed on the website services. However, the risk for abuse of the website users' personal or payment data remains.

Customer Incentives:

The vendor has a pricing strategy encouraging longer binding subscription periods by reducing the monthly price. A free trial is offered upon request.

Illegal IPTV Subscription

Case study number 7: Suspected unauthorised IPTV subscription selling website

Date of analysis: 01/03/2019 - 21/06/2019

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Unauthorised IPTV subscription vendors offer access to numerous multinational TV channels. Usually they provide high quality streaming. Websites may vary in their social-media presence, pricing strategies and IPTV content provided. Some vendors include access to vast video on demand libraries (movies, TV series). Most websites present a user-friendly interface and are simple to use.

To access the service, customers have to pay a monthly subscription fee. Subscription period normally is for 1, 3, 6, or 12 months. An attractive feature is that there is no binding contract period. Payments can be made with credit or debit cards, or through PayPal accounts. Some vendors also accept payments with crypto currencies (e.g. Bitcoin). Most websites have a customer support function and queries can be made through email or live-chat. Due to their overall design, user interface and customer support, these websites may be easily confused with a legitimate service. Websites are categorised as a non-deceptive business model. Revenues are made from direct sales of subscriptions.

Matrix	Online Digital Platform	A	B	C	D	E	F
		Internet Site Controlled by Infringer	Third Party Marketplace	Social Media or Blog	Gaming or Virtual World	E-mail, Chatroom or Newsgroup	Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology:	Products and Services:	Involved IPR(s):
Open internet. IPTV services are accessible to registered users for a fee.	The website offers streaming access to 45 UK and Irish TV channels. Interestingly, the site provides many unrelated services such as real estate maintenance and car-hire. The peculiar website domain is suspected to act as a disguise and hide potentially unlawful IPTV services. Prices start as low as a EUR 1 daily fee, or EUR 35 monthly charge.	Copyright and related rights
Identification of Infringer:	Revenue Sources:	Customer Relations:
The IP address location is identified to be in the United Kingdom. The registrar country is Portugal. Name and address of the registrant can be identified through the domain name registry WHOIS information.	Revenue is generated from direct sales of suspected unauthorised IPTV subscriptions. The vendor does not provide any information on accepted payment methods. Any purchase is through direct contact via phone or the email indicated.	The service has no binding subscription period – it appears that clients can choose to subscribe to the service for a period as brief as one day. The contact details indicated by the vendor is an address in Portugal, landline and mobile phone numbers and an email address. The website does not describe any usage restrictions or limitations. Based on this, it appears the service is available worldwide.
Resilience Against Enforcement Action:		
N/A		
Marketing Channels and Internet Traffic Features:		
The website has no social accounts. This potentially illicit business model might be directed at UK and Irish ex-pats in Portugal.		Users are well informed on the website services. However, the risk for abuse of the website users' personal or payment data remains.
Customer Incentives:		
A free demonstration version of the services is promoted. It is accessible upon direct contact with the vendor.		

Illegal IPTV for Resellers

Case study number 8: Suspected unauthorised IPTV panel for resellers

Date of analysis: 01/03/2019 - 21/06/2019

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Unauthorised IPTV vendors sell access to servers and streaming packages for numerous TV channels. Payments are charged as monthly subscriptions. Customers can further sell the IPTV streaming service to multiple individuals. For this reason, this is identified as a business-to-business (b2b) model.

To access their service, users must register and purchase a certain amount of 'credits' to start accessing the live channel streams. Normally, one credit equals one euro. Payments are made through PayPal or credit and debit cards. Payments in Bitcoin are encouraged via a discount.

Explicit tutorials are provided that explain how to set up a website to offer IPTV services, manage customers and payments. The website interface is simple and user-friendly.

The websites are categorised as a non-deceptive business model. Revenues are made from reseller subscription payments.

Matrix

Online Digital Platform

AInternet Site
Controlled by
Infringer**B**Third Party
Marketplace**C**Social Media or
Blog**D**Gaming or
Virtual World**E**E-mail,
Chatroom or
Newsgroup**F**

Mobile Devices

1 Domain Name or Digital Identifier Misuse of IPR

A1

B1

C1

D1

E1

F1

2 Physical or Virtual Product Marketing

A2

B2

C2

D2

E2

F2

3 Digital Content Sharing

A3

B3

C3

D3

E3

F3

4 Account Access or Codes to Digital Content Sharing

A4

B4

C4

D4

E4

F4

5 Phishing, Malware Dissemination or Fraud

A5

B5

C5

D5

E5

F5

6 Contributing to Infringement

A6

B6

C6

D6

E6

F6

Digital Platform & Technology:

Open internet.
Services are accessible to registered users for a fee.

Products and Services:

Website offers streaming access to more than 12 000 TV channels, categorised into packages by language type (e.g. German, Turkish, Russian) or content (Mix, Adult, Sports, and VoD movies). These channel packages are sold to be further streamed to multiple individual users. Additionally, vendor sells unauthorised IPTV subscriptions to direct users.

Involved IPR(s):

Copyright and related rights.

Identification of Infringer:

Registrant country is Tunisia. In-depth investigation shows the IP address in the Netherlands. The registrant name and address can be identified through the domain name registry WHOIS information.

Revenue Sources:

Revenue is generated from IPTV package sales to resellers of unauthorised IPTV subscriptions. Payments are made with credit cards. Technical analysis found that payments are made through 'mule' companies.

Customer Relations:

The service has no binding period. Instant delivery is upon subscription payment. The website does not describe any usage restrictions or limitations. Based on this, it appears the service is available worldwide.

Resilience Against Enforcement Action:

N/A

Users are well informed on the website services. However, the risk for abuse of the website users' personal or payment data remains.

Marketing Channels and Internet Traffic Features:

The website runs its blog in Arabic where it shares cinema and sports news.

Customer Incentives:

The pricing strategy encourages longer binding subscriptions, e.g. an annual one user cost is 75 credits (6.25 monthly), while a single month access costs 10 credits.

Illegal IPTV for Resellers

Case study number 9: Suspected unauthorised IPTV panel for resellers

Date of analysis: 01/03/2019 - 21/06/2019

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Unauthorised IPTV vendors sell access to servers and streaming packages for numerous TV channels. Payments are charged as monthly subscriptions. Customers can further sell the IPTV streaming service to multiple individuals. For this reason, this is identified as a business-to-business (b2b) model.

To access their service, users must register and purchase a certain amount of 'credits' to start accessing the live channel streams. Normally, one credit equals one euro. Payments are made through PayPal or credit and debit cards. Payments in Bitcoin are encouraged via a discount.

Explicit tutorials are provided that explain how to set up a website to offer IPTV services, manage customers and payments. The website interface is simple and user-friendly. The websites are categorised as a non-deceptive business model. Revenues are made from reseller subscription payments.

Matrix

Online Digital Platform

A

Internet Site Controlled by Infringer

B

Third Party Marketplace

C

Social Media or Blog

D

Gaming or Virtual World

E

E-mail, Chatroom or Newsgroup

F

Mobile Devices

1 Domain Name or Digital Identifier Misuse of IPR

A1

B1

C1

D1

E1

F1

2 Physical or Virtual Product Marketing

A2

B2

C2

D2

E2

F2

3 Digital Content Sharing

A3

B3

C3

D3

E3

F3

4 Account Access or Codes to Digital Content Sharing

A4

B4

C4

D4

E4

F4

5 Phishing, Malware Dissemination or Fraud

A5

B5

C5

D5

E5

F5

6 Contributing to Infringement

A6

B6

C6

D6

E6

F6

Digital Platform & Technology:

Open internet. Services are accessible to registered users for a fee.

Products and Services:

Website offers streaming access to more than 10 000 TV channels as well as 3 000 VoD online access. TV channel packages are sold as a product to be used to provide further streaming services to multiple individual users.

Involved IPR(s):

Copyright and related rights.

Identification of Infringer:

The IP address is located in Bulgaria. Website owner information is protected by a third-party company which registered the DNS. The registrant country is identified in Panama through the domain name registry WHOIS information.

Revenue Sources:

Revenue is generated from IPTV package sales to resellers of unauthorised IPTV subscriptions. Payments are made via PayPal or with Bitcoin. A 1-month reseller subscription costs EUR 6 (3 credits).

Customer Relations:

The service has no binding period. The subscription period varies and a reseller can opt for 1-month, 3-month, 6-month or 1-year subscription. Instant delivery is upon subscription payment. The website does not describe any usage restrictions or limitations. Based on this, it appears the service is available worldwide. The website offers 24/7 customer support. Contact details such as WhatsApp, Skype, a phone number, Email and a mailing address are made available.

Resilience Against Enforcement Action:

The domain 'x.net' was de-indexed by Google in November 2018. Service continues to operate under '.com' and various other TDN.

Marketing Channels and Internet Traffic Features:

The website has Facebook and Twitter social accounts. The website also communicates via a newsletter that is sent out to registered email addresses.

Users are well informed on the website services. However, the risk for abuse of the website users' personal or payment data remains.

Customer Incentives:

The pricing strategy encourages longer binding subscriptions, e.g. annual re-seller subscription per user costs 25 credits (EUR 4.17 monthly), while a single month access costs EUR 6.

Illegal IPTV for Resellers

Case study number 10: Suspected unauthorised IPTV panel for resellers

Date of analysis: 01/03/2019 - 21/06/2019

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Unauthorised IPTV vendors sell access to servers and streaming packages for numerous TV channels. Payments are charged as monthly subscriptions. Customers can further sell the IPTV streaming service to multiple individuals. For this reason, this is identified as a business-to-business (b2b) model.

To access their service, users must register and purchase a certain amount of 'credits' to start accessing the live channel streams. Normally, one credit equals one euro. Payments are made through PayPal or credit and debit cards. Payments in Bitcoin are encouraged via a discount.

Explicit tutorials are provided that explain how to set up a website to offer IPTV services, manage customers and payments. The website interface is simple and user-friendly. The websites are categorised as a non-deceptive business model. Revenues are made from reseller subscription payments.

Matrix	Online Digital Platform	A	B	C	D	E	F
		Internet Site Controlled by Infringer	Third Party Marketplace	Social Media or Blog	Gaming or Virtual World	E-mail, Chatroom or Newsgroup	Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology:

Products and Services:

Involved IPR(s):

Open internet. Services are accessible to registered users for a fee.

The vendor offers streaming access to multiple international TV channels. The precise number of channels is not identified on the website. TV channel packages are sold as a product to be used to provide another streaming service to multiple individual users.

Copyright and related rights.

Identification of Infringer:

Revenue Sources:

Customer Relations:

The IP address is identified in the USA. The DNS is registered by a third-party company to disguise information on the website owner.

Revenue is generated from IPTV package sales to resellers of unauthorised IPTV subscriptions. Payments are made via PayPal or with Bitcoin, credit and debit cards are also accepted. A 1-month reseller subscription costs USD 6. There is additional USD 25 registration fee.

The service has no binding period. The subscription period varies and reseller can opt for 1-month, 3-month, 6-month or 1-year subscription. Instant delivery is upon the subscription payment. The website does not describe any usage restrictions or limitations. Based on this, it appears the service is available worldwide. Contact details such as a phone number, email and mailing address are made available.

Resilience Against Enforcement Action:

The website has been the object of various de-index requests to Google. However, it appears to still feature in search results.

Marketing Channels and Internet Traffic Features:

The website has a Twitter account. Access from VPN's is allowed.

Users are well informed on the website services. However, the risk for abuse of the website users' personal or payment data remains.

Customer Incentives:

The pricing strategy encourages longer binding subscriptions, e.g. an annual reseller subscription per user costs USD 40 (USD 3.3 monthly), while a single month access costs twice as much — USD 6. A refund option is made available in case of unsatisfactory service provision.

Case study number 11: Suspected unauthorised free IPTV streaming

Date of analysis: 01/03/2019 - 21/06/2019

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Unauthorised free IPTV providers facilitate access to copyright-protected TV channels. The users can browse through the website to find links that stream live TV broadcasts. External links may lead to different file sharing networks through which content could be downloaded. The website links section appears to be maintained thoroughly, each link verified and regularly updated.

Many operators have a social media presence and an online customer support function. Usually simple and explicit tutorials on free IPTV streaming (e.g. m3u file download or set top box install) are made available on these websites.

It has not been investigated whether the shared content or the advertising on these websites has malware. Therefore, it cannot be determined whether the business model is deceptive or not.

Matrix IPR Infringing Activity	Online Digital Platform	A	B	C	D	E	F
		Internet Site Controlled by Infringer	Third Party Marketplace	Social Media or Blog	Gaming or Virtual World	E-mail, Chatroom or Newsgroup	Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR		A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing		A2	B2	C2	D2	E2	F2
3 Digital Content Sharing		A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing		A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud		A5	B5	C5	D5	E5	F5
6 Contributing to Infringement		A6	B6	C6	D6	E6	F6

Digital Platform & Technology:

Open internet website with domain name under the generic top-level domain '.me'. The website has operated under other TDMs such as '.biz' and '.org'. It is a freely accessible website.

Products and Services:

The website offers links to live-streamed sports events on TV channels.

Involved IPR(s):

Copyright and related rights

Identification of Infringer:

The registrant country is identified as Australia. The IP address location is in the Czech Republic. No accessible record on the registrant or registrar is available. DNS is registered by a third-party company to disguise information on the website owner.

Revenue Sources:

Revenue comes from advertising and affiliated marketing. There exists a possibility for malware and revenue made from sales of user's information.

Customer Relations:

The website maintains an up-to-date catalogue of links to copyright protected content. A community-based discussion and comments forum is available as a way to engage customers.

Resilience Against Enforcement Action:

The website and its owner have been subject to legal proceedings in Italy, Spain and France. The website has been blocked by court orders in the UK and France, and by administrative orders in Italy.

The business model could be deceptive if the website uses malware against its users. It appears that the content and means of access are clearly described in connection to the links.

Marketing Channels and Internet Traffic Features:

The website has social media accounts on Facebook and Twitter. Any member can post stream links under specific terms. Members can post their content for revenue.

Customer Incentives:

Free access to live sports events broadcast by TV channels.

Case study number 12: Suspected unauthorised free IPTV streaming

Date of analysis: 01/03/2019 - 21/06/2019

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Unauthorised free IPTV providers facilitate access to copyright-protected TV channels. The users can browse through the website to find links that stream live TV broadcasts. External links may lead to different file sharing networks through which content could be downloaded. The website links section appears to be maintained thoroughly, each link verified and regularly updated. Many operators have a social media presence and an online customer support function. Usually simple and explicit tutorials on free IPTV streaming (e.g. m3u file download or set top box install) are made available on these websites. It has not been investigated whether the shared content or the advertising on these websites has malware. Therefore, it cannot be determined whether the business model is deceptive or not.

Matrix	Online Digital Platform	A	B	C	D	E	F
		Internet Site Controlled by Infringer	Third Party Marketplace	Social Media or Blog	Gaming or Virtual World	E-mail, Chatroom or Newsgroup	Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology:	Products and Services:	Involved IPR(s):
Open internet website with domain name under the generic top-level domain '.com'. Content is freely accessible.	The portal offers free live online TV broadcasts (over 800 channels). Users of PCs and other consumer electronic devices can easily find and access IPTV and other streaming media content. This site contains several links to third-party sites.	Copyright and related rights
Identification of Infringer:	Revenue Sources:	Customer Relations:
The registrant country is identified as the Netherlands through the domain name registry WHOIS information. The server location could not be identified reliably as it is hosted by 'Cloudflare'. DNS is registered by a third-party company to disguise information on the website owner.	Revenue comes from advertising and affiliated marketing. There exists a possibility of malware and revenue made from sales of user information.	The website maintains an up-to-date catalogue of links to copyright protected content. The business model could be deceptive if the website uses malware against its users. It appears that the content and means of access are clearly described in connection to the links.
Resilience Against Enforcement Action:		
N/A		
Marketing Channels and Internet Traffic Features:		
The website has social media accounts on Facebook and Twitter. It is possible to add a new TV station or a streaming event by getting in contact via the indicated email.		
Customer Incentives:		
Free access to multiple international live TV channel broadcasts.		

APPENDIX III — ECOSYSTEM OF ILLEGAL IPTV

ILLEGAL IPTV IN THE EUROPEAN UNION

RESEARCH ON ONLINE BUSINESS MODELS INFRINGING INTELLECTUAL PROPERTY RIGHTS — PHASE 3

Report

