Study on Legislative Measures Related to Online IPR Infringements

A Project Commissioned by the European Union Intellectual Property Office

Riis, Thomas; Elholm, Thomas ; Nordberg, Ana; Schwemer, Sebastian; Wallberg, Knud

DOI:
10.2814/36519

2018

Document Version:
Publisher's PDF, also known as Version of record

EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE IPR INFRINGEMENTS

A PROJECT COMMISSIONED BY THE EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE IPR INFRINGEMENTS

Project team

Thomas Riis, LL.D., PhD, Professor of Law, Centre for Information & Innovation Law, University of Copenhagen
Thomas Elholm, PhD, Professor of Law, Department of Law, University of Southern Denmark
Ana Nordberg, PhD, Associate Senior Lecturer, Faculty of Law, Lund University
Sebastian Schwemer, PhD, PostDoc, Centre for Information & Innovation Law, University of Copenhagen
Knud Wallberg, PhD, PostDoc, Centre for Information & Innovation Law, University of Copenhagen

ISBN 978-92-9156-256-5 doi:10.2814/819909 TB-04-18-425-EN-N

CONTENT

1. FOREWORD

Infringements of intellectual property rights have been on the rise over a number of years. But especially in the area of online infringements the tendency has been very significant.

The EUIPO has previously published reports about how infringements in the online environment are carried out, what business models are applied by the infringers and other relevant facts about the problem.

Online infringements of intellectual property rights and other internet borne illegalities and criminal activities, however, cannot be seen isolated from the possible legal responses.

To counter the different problems of criminality on the internet, a number of legislative measures have been taken. And often existing legislative measures known from the physical world have been applied in the online environment. Sometimes legislative measures are specifically targeting a specific area of online illegality, sometimes they are more general.

The EUIPO has previously described the legal situation in regards to a number of issues related to protection and enforcement of intellectual property rights, but the special issues raised by the online environment needed to be explored further.

For this report it was the intention to take a cross-sectorial view at enforcement of intellectual property rights on the internet, covering civil, administrative and criminal enforcement.

The aim has been to develop a practical problem-oriented description of legal measures. Therefore, in this study eight specific — and practically relevant topics — have been identified as key areas.

The report provides a legal overview, but does not aim to provide the full picture of legal measures available in the EU Member States to counter infringements of intellectual property rights online. However, the EUIPO is determined to follow up this study with further in-depth studies of specific legal issues.

And the EUIPO will continue to be dedicated to develop, support and implement cross-sectorial and innovative ways to describe, analyse and spread best practices utilised in the online environment, including legal measures.

2. EXECUTIVE SUMMARY

Background

Intellectual property right (IPR) infringement has taken and increasingly takes place in the online environment, in particular on the internet, which has raised concerns on many different levels, and has led to a number of recent European initiatives[1].

A number of legislative measures have been adopted at both international and European levels whose purposes are to strengthen and harmonise the protection of IPR. These measures include remedies, which aim to enable rights holders and law enforcement authorities, such as prosecutors, to enforce IPR in an effective manner[2].

However, the provisions in the abovementioned legislation are, for the most part, not drafted in ways that specifically address how to prevent or combat online IPR infringement, but are -merely in the form of minimum requirements, which leave room for individual Member States to adopt and apply specific national measures.

Previous Observatory studies have looked into IPR infringement in the online environment, but none of them have dealt with the issue as to which concrete, existing, legislative measures can be used to prevent or combat online IPR infringement[3].

The main purpose of this study is, therefore, to establish whether and to what extent a number of *specific* legislative measures, which can be applied to prevent or combat IPR infringement in the online environment, are available in the Member States. The legislative measures that the study will focus on are measures that can be characterised as providing 'practical solutions to practical problems', such as the option to require that an online service provider discloses the identity of a customer who is suspected of infringing the IPR rights of a third party and the option to apply the European Investigation Order (EIO) to crimes involving IPR.

[1] Most notably, the 2013 Europol's Serious and Organised Crime Threat Assessment (SOCTA), the EU Customs Action Plan to combat IP infringements for the years 2013-2017, the Commission Communication on a Digital Market Strategy for Europe (COM(2015) 192 final) and the joint Europol and EUIPO Situation Report on Counterfeiting in the EU, the latest report being form 2017.

[2] See the overview of these legislative measures below in Chapter 7.

[3] Reference will however, be made to the related study: Study on voluntary collaboration practices in addressing online infringements of trade mark rights, design rights, copyright and rights related to copyright, 2016.

Methodology

The main purpose of this study is to establish whether a number of specific legislative measures, which may be used to combat or prevent online IPR infringement, are in fact available in the EU Member States, and if so whether they have been or can be applied for this purpose in each Member State.

To fulfil this goal, the initial part of the study consisted of mapping the available legislative measures in relation to the following eight selected topics:

1	Obtaining account information
2	Blocking access to websites
3	Domain name actions
4	Actions targeted at hosts
5	European Investigation Order
6	Extradition – European Arrest Warrant
7	Money laundering
8	Criminal sanctions

The main tools for the mapping exercise consisted of two questionnaires: one addressed civil measures and one addressed criminal measures.

The questionnaires were presented to an expert group that was established for this study, after which it was sent out to representatives of all Member States through two different practitioner networks.[4]

Most of the detailed questions received replies and from most, albeit not all, Member States[5], which is a fact that must be taken into account when reading the study. However, since the aim of mapping was to draw the overall picture of the availability of legislative measures in the EU Member States as such rather than a detailed picture of the situation in each Member State[6], the number of replies justifies that it is possible to draw this overall picture.

[4] The questionnaire on civil measures was distributed to a number of individual ECTA members and ECTA Committee members. The questionnaire on criminal measures was sent to the various national authorities that are represented in EUROJUST. The project team wishes to thank all of the respondents for their valuable and essential contributions to the study.

[5] The number of missing replies will be indicated in each table as “No answers”.

[6] An example of a study which focuses on the legal situation in each Member State is the EUIPO report ‘Consumers Frequently Asked Questions (FAQS) on Copyright’, 2017, available at: https://euipo.europa.eu/ohimportal/da/web/observatory/observatory-publications

Furthermore, it has been outside the scope of the study to verify the replies independently. The replies thus reflect the views of the respondents, which must be borne in mind when reading the study in general, and in particular when individual responses have been quoted or highlighted.

Key findings

The mapping and analysis of the legislative measures that are available in the responding EU Member States, and which can be used by the rights holders and the competent authorities to combat and prevent online IPR infringement, show both EU-wide commonalities and national differences.

In relation to the first two of the abovementioned eight topics, namely the legislative measures that concern the disclosure of information on a suspected infringer and the possibility to block access to websites, these measures are as a starting point available in all Member States[7]. In addition, the legal basis for the diverse national measures has been harmonised to a certain extent by the relevant articles in the Directive on the enforcement of IPR[8]. Although the fundamental conditions for obtaining such information or for achieving a blocking order are to some degree harmonised, differences between the Member States may exist when it comes to the more detailed, procedural conditions. In most Member States, harmonised legislation is thus complemented by specific, national legislation, such as the general laws on civil and criminal procedures, whose provisions also apply to both IPR infringement and other kinds of illicit behaviour[9].

As regards the third topic on domain name actions, the picture is notably different. The EU has not harmonised national legislation on registration and administration of the country code top-level domains (ccTLDs) of the individual Member States. This means that the legal basis for the specific legislative measures that this study covers — namely suspension, transfer or deletion of domain name registrations that are suspected of infringing the IPR of a third party — is subject to the national laws of each Member State and to the specific rules or user terms that the administrator of each ccTLD has laid down. Although the three analysed legislative measures are available in most Member States, none of them are available in all Member States. By way of an example, in some Member States it may be possible to obtain a court order that transfers infringing domain names from the holder of the domain names to the rights holder. This will not be possible in other Member States, even if the involved parties are the same.

The mapping and analysis of the fourth topic on legislative measures aimed at the entities that host suspected IPR infringing content, also reveals a rather fragmented, overall picture. On the one hand, the exemption from liability of hosting providers is covered by Article 14(1) of the Directive on electronic commerce[10], which is implemented into the laws of all Member States. However, the actual standard of

[7] There are some amendments to this starting point in certain situations. See more details in Chapters 8.2 and 8.3.

[8] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

[9] As regards disclosure of information, the situation has been aptly described as ‘a mosaic approach that requires the courts to apply different national laws’, by Roland Knaak and Lukasz Zelechowski in Michel Vivant (ed.): ‘European case-law on infringements of intellectual property rights’, Bruylant, 2016.

[10] 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 (OJ L 178, 17 July 2000).

secondary liability is not harmonised and thus relies on national law. Article 14(1) of the Directive on electronic commerce implies that the provider is not liable for the content that it hosts for its customers, unless the host knew that the content was illegal or does not act expeditiously to 'take down' (i.e. to remove or disable access to) the content as soon as it is made aware of the illegal content. Thus, while a hosting provider is not liable typically for infringing material, it is possible to get a court order that requires a host to take down IPR infringing content from its platform in all Member States. On the other hand, the option to require that a host provider suspend the existing account of a suspected infringer is not subject to specific EU legislation, and mapping shows that this legal measure is either unavailable or the availability is unresolved in almost half of the Member States. The situation is even more fragmented when it comes to the option to prevent a suspected infringer from opening a new account with the hosting service when an account has been suspended previously. This legal measure is either unavailable or its availability is unclear or subject to legal debate in over half of the Member States.

IPR infringement in the digital environment implies that the infringing activities may take place in several Member States simultaneously, while the suspected infringers may be located in one or several Member States. Investigative judicial cooperation between the Member States, therefore, plays an important role in IPR enforcement in such cases.

The EIO[11] is a recent legislative measure of judicial cooperation between the Member States that replaces a previously more fragmented framework[12]. It is based on mutual recognition of decisions, which means that each Member State is obliged to recognise and carry out the request of another Member State, as it would do with a decision coming from its own authorities. Counterfeiting and product piracy is included in the list of offences, which are covered by the EIO if the basic requirement of the EIO is met, namely that the offence is subject to *a* maximum period of at least three years imprisonment in the issuing country. However, not every type of IPR infringement is considered to be 'counterfeiting and piracy', and the maximum sentence in cases of counterfeiting and piracy is not three years in all Member States. Both of these factors limit the application of the EIO by the competent authorities in the Member States in relation to IPR infringement.

The European Arrest Warrant (EAW)[13] is a simplified cross-border procedure for prosecuting or executing a custodial sentence or detention order. An EAW is a request issued by a judicial authority in one Member State to detain a person located in another Member State and to surrender the said person for prosecution in the requesting Member State. 'Counterfeiting and piracy of products' as well as 'computer related crimes' are included in the list of offences, which do not require that the offence is also a criminal act in the executing state. This is a derogation from the otherwise existing requirement of 'double criminality', meaning that the offence that forms the background for the EAW is punishable in

[11] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the European Investigation Order in criminal matters, (EIO Directive).

[12] The EIO is intended to create a comprehensive system to replace all the existing instruments in this area, including Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for obtaining objects, documents and data for use in proceedings in criminal matters, and it should cover 'as far as possible all types of evidence, containing time-limits for enforcement and limiting as far as possible the grounds for refusal' (Recital 6, EIO Directive).

[13] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18 July 2002.

both the issuing state and in the executing state. It is, however, a condition that the offence is punishable by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined by the law of the issuing Member State[14]. Similarly to the abovementioned EIO, such limitation precludes the application of the EAW in some Member States for a number of IPR infringements. In such cases an EAW may, however, still be issued if the IPR infringement is punishable in the issuing Member State with at least 12 months of imprisonment, in addition to which the executing State may then require that the criminal offence, on which the EAW is based, also constitutes an offence under their national law.

The two most recently adopted anti-money laundering instruments, namely, 'The Fourth Anti-Money Laundering Directive'[15] and 'The Fund Transfers Regulation'[16], cover proceeds originating from most types of criminal activities[17]. The instruments, in principle, cover proceeds originating from online IPR infringement, but at present there appear to be no concrete examples of this.

The study also addresses a number of aspects that relate to criminal sanctions in the event of IPR infringement, which are laid down in the national laws of the Member States. Criminal sanctions are not subject to harmonisation at EU level, but as is illustrated above, the type of penalties and the maximum penalties do at the same time play an important role in the actual applicability to online IPR infringement of the two EU, law-based legislative measures, the EIO and the EAW. Mapping shows that the type of penalties and the maximum penalties for IPR infringement vary considerably in the Member States, namely maximum custodial sentences, where those are applicable, which vary from 2 to 10 years. Furthermore, when it comes to such issues as whether negligent infringements are punishable and whether legal persons can be held liable for criminal infringements, the legal situation in the Member States is far from uniform.

A separate chapter contains some concluding observations on the analysis and also suggests that there is room for and need for more in-depth studies on a number of the discussed topics.

Technological advancements have had an impact, and are likely to continue to impact both online IPR enforcement as well as possible IPR infringement. The final chapter identifies a number of these new opportunities and challenges, such as the use of blockchain technology, the use of big data and filtering techniques and the privatisation of enforcement mechanisms through the use of non-judicial takedown mechanisms.

---

[14] Article 2(2) EAW Council Framework Decision.

[15] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Money Laundering Directive.)

[16] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (text with EEA relevance), OJ L 141, 5 June 2015, pages 1-18.

[17] See the definition of 'criminal activities' in Article 3(4) of the Money Laundering Directive and, in particular, the definition of 'offences' in Section (f).

3. BACKGROUND AND PURPOSE

It is well known that a large and ever increasing part of trade in the EU takes place in the online environment. According to recent figures from Eurostat, about 68 % of internet users in the EU shopped online in 2017[18]. The same trend is notable when it comes to the use of the internet by rights holders to distribute digital content[19], such as movies, series, music and sports events. The growth in the use of the internet for legitimate trade and distribution is, however, being paralleled by a growth in the number of infringements of intellectual property rights (IPR), which has raised concerns on many different levels and has led to a number of recent European initiatives[20].

Previous Observatory studies have looked into IPR infringements in the online environment, most recently the Research on Online Business Models Infringing Intellectual Property Rights[21] that in Phase 1 identified known business models used to infringe IPR online and in Phase 2 made an in-depth study of one of these business models. Neither of these studies, nor other of the Observatory studies do, however, deal with the issue of which of the existing legislative measures which can be used to prevent or combat online infringements of IPRs[22].

A number of legislative instruments have been adopted at international, European and national levels whose purposes are to facilitate and strengthen the enforcement of IPRs. These legislative measures include remedies enabling rights holders or law enforcement authorities, such as police and prosecutors, to enforce IPRs in the online environment[23].

However, the provisions in these legislative instruments are often drafted in general terms that do not specifically address how to prevent or combat online infringements of IPRs. Moreover, the instruments

[18] Published at http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals#68.C2.A0.25_of_internet_users_in_the_EU_shopped_online_in_2017

[19] See, inter alia, paragraphs 2.4 and 3.2 in COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A Digital Single Market Strategy for Europe.

[20] Most recently, the European Commission Communication: — Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights, 29 November 2017 (COM(2017) 708). Reference is also made to the European Commission: Communication on Tackling Illegal Content Online — Towards an enhanced responsibility of online platforms, 28 September 2017 (COM(2017) 555 final), the Commission Communication from a Digital Single Market Strategy for Europe (COM(2015) 192 final) and the joint Europol and EUIPO Situation Report on Counterfeiting in the EU, the latest report being from 2017.

[21] Research on Online Business Models Infringing Intellectual Property Rights, Phase 1, EUIPO, 2016 and Phase 2, EUIPO, 2017, available at: https://euipo.europa.eu/ohimportal/da/web/observatory/observatory-publications

[22] Reference will, however, be made to the related study: Study on voluntary collaboration practices in addressing online infringements of trade mark rights, design rights, copyright and rights related to copyright, 2016.

[23] See the overview of these legislative measures below in Chapter 7.

set the minimum level of protection, and do thus not intend to fully harmonise or align the **legislative** measures that can be applied to combat IPR infringements. Consequently, EU Member States may to some extent adopt, implement and apply specific national legislative measures or apply existing legislative measures to IPR infringements, too.

The main purpose of this study is, therefore, to establish whether and to what extent a number of *specific* legislative measures, which can be applied to prevent or combat infringements of IPR's in the online environment, are available in the Member States. The study will focus on measures that can be characterised as providing 'practical solutions to practical problems', such as the possibility to require an online service provider to disclose the identity of a customer that is suspected to infringe the IPRs of a third party or the possibility to apply the EIO[24] on crimes involving IPRs. These practical legislative measures were identified in the initial phase of the study as being of particular interest in this context, and they have been linked to the following eight horizontal topics:

1	Obtaining account information
2	Blocking of access to websites
3	Domain name actions
4	Actions targeted at hosts
5	EIO
6	Extradition – EAW
7	Money laundering
8	Criminal sanctions

The specific measures as well as the eight topics will be explained and analysed below in Chapter 8 of the study.

[24] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the EIO in criminal matters.

4. METHODOLOGY

The main purpose of the study is to establish whether and to what extent a number of identified legislative measures that can be used to prevent and combat online IPR infringements are available in the EU Member States.

In order to fulfil this goal, the initial part of the study consisted of mapping the available legislative measures in relation to the eight selected topics. The main tools for the mapping exercise were two questionnaires: one questionnaire that addressed civil measures (see Annex 1) and one that addressed the criminal measures (see Annex 2).

The questionnaire on civil measures included the first four of the eight topics, while the questionnaire on criminal measures included all eight topics. For each topic, the respondents were asked to reply to various specific questions that address situations that frequently occur in practice in cases dealing with online infringements of IPRs.

The questions were phrased using wording such as: 'Can [a specified defendant] be ordered to [perform a specific action]?' This wording was used to reflect the fact that the decisive test for whether a specific legal measure is available or not, is that a court or other competent authority may ultimately order the defendant to implement a certain action (or omission). This does not, however, mean that the legislative measures cannot be and indeed are being applied outside of court proceedings. An illustrative example of this is the widespread application by online intermediaries of voluntary 'takedowns' of infringing websites and sales offers based on notices filed by the rights holders[25].

For each question, the respondents could tick one of the following four boxes: 'yes'; 'yes, but only under certain circumstances'; 'no' or 'unresolved', just as they were asked to reason their answers.

The respondents were also given the opportunity to make any other remarks or comments on the eight issues, other than those that were addressed in the detailed questions.

The questionnaires were presented to an expert group that was established for this study[26].The questionnaires were then sent out to representatives of all Member States through networks of practitioners, and replies were received from most of the Member States[27]. For statistical comparison

[25] Knud Wallberg: 'Notice and takedown of counterfeit goods in the Digital Single Market: a balancing of fundamental rights', Journal of Intellectual Property Law & Practice, Volume 12, Issue 11, 1 November 2017, pages 922-936.

[26] The Expert Group consisted of representatives from the following public sector organisations: EUROJUST, the EU Commission (DG Grow), Uppsala University and WIPO (observer), and from the following private sector organisations: AAPA, BASCAP, INTA and SACG.

[27] The questionnaire on civil measures was distributed to a number of individual ECTA members and ECTA Committee members. The questionnaire on criminal measures was sent to the various national authorities that are represented in EUROJUST. We thank both organisations and the individual respondents for their indispensable contributions.

purposes, absent replies were taken into account and distinguished from purposely blank answers, which may denote for example either, lack of relevance of the question, or lack of information on the subject in the respective jurisdiction.

Answers were accrued exactly as received, and in our overall analysis the qualitative comments of respondents and legal sources invoked were given prevailing consideration.

The replies to the questionnaires have formed the primary basis for the analyses and thus for the outcome of the study. The replies reflect the views and factual knowledge of the respondents. Given the primary practical approach to the issues that are dealt with in the report, such knowledge was presumed to be accurate and updated, and it has been beyond the scope of the analyses to conduct in-depth verifications of the replies. Therefore, the individual responses quoted in the report have to be read taking this into consideration.

5. DEFINITIONS AND DELIMITATIONS

Intellectual property rights (IPRs): The term covers a number of exclusive rights including but not limited to trade marks, copyrights and related rights, protected unoriginal databases, design rights, patents, utility models, geographical indications, topography of semiconductors, plant variety rights, and trade names, in so far as they are protected as exclusive property rights in the national law concerned. The study will, however, focus on infringements of copyrights and related rights and trade marks, so unless it is stated otherwise the term will only cover those rights.

Online infringements: The study deals with infringements that take place on the open part of the internet[28] and the primary focus is on infringements of a commercial scale, meaning that the infringing acts are 'carried out for direct or indirect economic or commercial advantage'[29]. The use of terms online and online environment in this report include any activity on the open internet, including websites, lower level pages, user profiles on social networking websites, online auction and trading platforms, email and internet connected applications on mobile devices.

Intermediaries: Internet intermediaries are entities — usually companies — that bring together or facilitate transactions between third parties on the internet. They give access to, host, send or index content, products and services originated by third parties on the internet or provide internet-based services to such third parties[30].

Domain name: The domain name system (DNS) serves the essential and central function of facilitating the internet users' ability to navigate the internet[31]. A domain name is the user-friendly address of a specific computer's underlying numeric IP address (see definition below). The domain name 'euipo.europa.eu' for example is tied to the computer with the numeric IP address 109.232.208.177, which means that instead of remembering and typing in '109.232.208.177' in the internet browser an internet user can type in 'euipo.europa.eu' to be connected to the EUIPO website.

Technically, the DNS works through a network of distributed databases that are operated by the designated *domain name registries*. These databases contain the lists of domain names and their

[28] The study will, therefore, not cover activities on the un-indexed parts of the internet, often referred to as the darknet. See the definition of 'darknet' on p. 14 in 'Research on Online Business Models Infringing Intellectual Property Rights. Phase 1. Establishing an overview of online business models infringing intellectual property rights', EUIPO, July 2016.

[29] As defined in Recital 14 of Directive 2004/48 on the enforcement of intellectual property rights. The study will thus not focus on infringements of copyrights and related rights that are committed by private persons as such.

[30] https://www.oecd.org/internet/ieconomy/44949023.pdf

[31] It is the internet Corporation for Assigned Names and Numbers (ICANN) that coordinates the key technical functions of the DNS and defines policies for how the 'names and numbers' of the internet should run.

corresponding IP-numeric addresses and perform the function of mapping the domain names to their numeric IP addresses for directing requests to connect computers on the internet.

Domain names must be registered with the *registry*[32] that is responsible for the specific top-level domain, and registrations have to be filed through an accredited domain name *registrar*. By way of an example, if a company wants to register an .eu domain name the company must contact an accredited .eu registrar and request the registrar to file an application to register the domain name on the company's behalf. If the domain name is vacant and all other formalities are fulfilled the domain name will be registered and entered into the .eu DNS database.

All domain names will be connected to one or more domain name servers, which is a 'computer server that contains a database of public IP addresses and their associated hostnames, and in most cases, serves to resolve, or translate, those common names to IP addresses as requested'[33]. The DNS servers are operated by entities who are authorised to do so by the registries — often referred to as 'name server managers' (DNS managers). Many of the accredited registrars are also authorised to operate as DNS managers.

The registries do not examine the applications for a new domain name against prior rights of third parties such as trade marks, company names or personal names. Third party rights holders are therefore compelled to enforce their rights after the domain name has been registered, if they find that a registered domain name infringes their rights[34].

IP address: the term is an abbreviation of internet protocol address, which is an identifier that is assigned to each computer or other device (e.g. a mobile device) that is connected to the internet or to another network using the TCP/IP protocol. The IP address is used to locate and identify the device in communications with other devices on the network.

An IP address may be static which means that the address will be the same each time the user uses its account with the provider to connect to the internet. A dynamic IP address means that the access provider will assign one of the IP addresses that it has available in its 'address pool' to the user when he or she logs on, but the said IP address will only be assigned for a limited amount of time, namely for the particular session. The IP address may subsequently be assigned to a new user[35]. It is determined in the agreement between the user and its access provider, which type of IP address that will be applied for the devices that are covered by a service agreement. However, mobile devices such as laptops, tablets and mobile phones can be and are very often connected to the internet via an access provider whose

[32] Many TLDs apply a shared registry model, in which case the registrars have access to register domain names directly in the registry database. The registry database is then administered by a dedicated registry administrator.

[33] As defined by LIFEWIRE, https://www.lifewire.com/what-is-a-dns-server-2625854

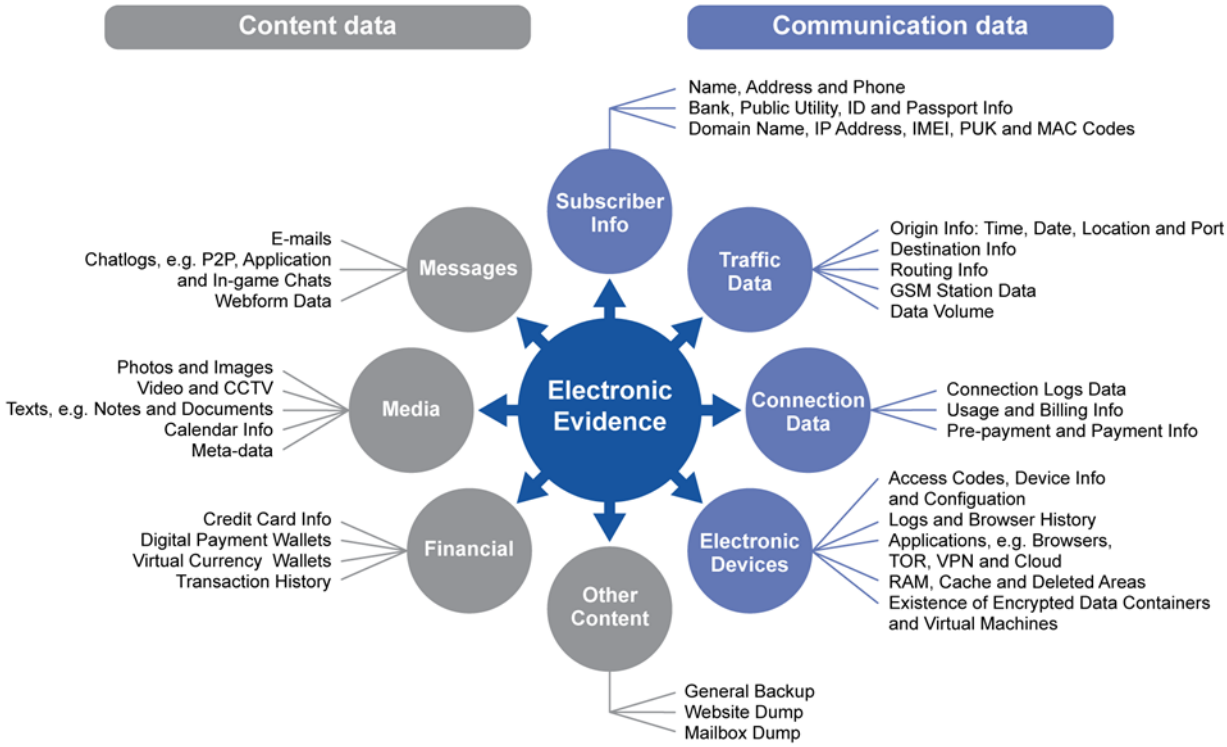
[34] Definition from the abovementioned 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016.

[35] Additional information on IP addresses can, inter alia, be found in the article 'What is a static IP-address?' https://www.lifewire.com/what-is-a-static-ip-address-2626012. The term 'address pool' originates from here.

services are available at the place where the user is currently located. Such services will typically use dynamic IP addresses[36].

Electronic evidence: Domain names and IP addresses are just two types of electronic evidence. As the figure below illustrates there are many other types of electronic evidence that may be relevant to collect in the particular cases that involve online infringements of IPRs.

FIGURE 1 — OVERVIEW OF DIFFERENT TYPES OF ELECTRONIC EVIDENCE



Civil law measures[37]: The body of legislative measures that is applicable in disputes between private entities.

Administrative law measures: The body of legislative measures that can be applied by administrative bodies.

[36] See Lasse Lund Madsen 'Edition som efterforskningsmiddel — med særlig henblik på internetrelaterede bedragerisager', ('Edition as investigative tool — with particular reference to internet related fraud cases'), U.2017B.205, p. 207.

[37] This distinction between these three different types of legal measures is traditionally used in many different contexts. Therefore, these terms will also be used in this study, although the terms are not necessarily used and construed in the same manner in all EU Member States. The study will not deal with the legal issues that arise from the interplay between the civil and criminal measures, such as the issue of self-incrimination.

Criminal law measures: The body of legislative measures that is applicable in cases of criminal investigations and prosecutions.

6. LISTING OF ONLINE INFRINGEMENTS OF TRADE MARKS, COPYRIGHTS AND RELATED RIGHTS OF PARTICULAR RELEVANCE FOR THE STUDY

IPR infringements in the online environment are diverse, both with regard to the 'content' of the infringement and to the technological means used[38]. The purpose of this chapter is solely to highlight those types of online infringements that are most relevant in relation to the issues that are addressed in the study. It does thus not intend to be exhaustive.

Illegal sharing and distribution of copyright protected works

The first and still widely applied way to distribute illegal copies of copyright protected works is through *file sharing*. File sharing is distributing or providing access to digital files such as computer programs, multimedia files, documents or e-books. In this context, digital files are files that include or consist of material protected by copyright or related rights. File sharing is carried out in a number of ways. While the original method involved manually sharing files that were copied on to a CD-ROM or similar movable storage devices, current methods take place online and include the use of dedicated file hosting servers of 'cyberlockers' or the use of peer-to-peer (P2P) networking[39].

In recent years, *streaming* has become a major means for copyright infringements; in particular, in relation to unauthorised streaming of live events such as sports games and concerts but also of popular series. Streaming is a technique for transferring data in a steady and continuous stream. With streaming, the client browser or plug-in can start displaying the data before the entire file containing the material has been sent[40], which is an advantage for those users that do not have access to the internet that is fast enough to download large multimedia files quickly.

[38] 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016.

[39] Wording based on the description of file sharing found at https://www.techopedia.com/definition/16256/file-sharing. See Canvas 24 in the abovementioned EUIPO study for a description of the use of 'cyberlockers' for IPR infringing activities.

[40] Based on the definition found at http://www.webopedia.com/TERM/S/streaming.html

Sale and distribution of IPR infringing goods

According to figures from Eurostat, about 65 % of internet users in the EU shopped online in 2015[41] and a large portion of this trade took place through known online marketplaces[42] It may also have taken place on social media platforms and through ordinary web shops, that is, web shops that operate under a dedicated domain name.

The growth in legitimate online trading is, however, being paralleled by a growth in illicit trade. Online marketplaces are thus being used by vendors to sell illicit goods such as pirated software and counterfeited clothes and mobile phones[43], and the same occurs on the social media platforms[44]. Also websites, which at first glance appear to be official websites of a particular brand owner, sometimes turn out to be bogus sites selling counterfeit goods. These websites often use domain names that include a third-party trade mark and the content and design of the website itself resembles that of the brand owner[45].

Fraud, extortion and other traditional cybercriminal offences

The abovementioned types of infringements of IPRs frequently[46] reach a scale where the infringements also constitute criminal offences, meaning that the penal provisions in the concerned national IPR legislation or in the penal code may apply.

In addition, trade marks are used for acts that are criminal offences from the outset, in particular in the widespread phishing scams. The term *phishing* is used to describe the malicious attempts to acquiring money or sensitive information or to install malware that is initiated through contact with victims achieved via emails, postings on social media platforms or blogs or via sms'. The inquiry will immediately appear to be sent in good faith and for a legitimate purpose: it will thus often appear to be sent by an established company since the sender address makes use of a domain name that resembles the genuine domain name of that company.

Spear phishing is an advanced and focused form of phishing that targets specific individuals and requires a larger and more focused effort from the attacker[47]. A recent variation of spear phishing is 'boss

[41] As referred to in the Digital Agenda Scoreboard, 2016 https://ec.europa.eu/digital-single-market/en/use-internet and available at http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals

[42] An overview of marketplaces across Europe can be found at: http://www.bvoh.de/overview-of-online-marketplaces-across-europe/ . A list of the top 20 marketplaces by traffic is listed on pages 17-18 in 'COMMISSION STAFF WORKING DOCUMENT: Online Platforms' {SWD(2016) 172}.

[43] An illustrative example can be found in Canvas 8 in 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016.

[44] An illustrative example can be found in Canvas 9 in 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016.

[45] See 'Research on Online Business Models Infringing Intellectual Property Rights — Phase 2 Suspected trade mark infringing e-shops utilising previously used domain names', EUIPO 2017.

[46] 2017 Situation Report on Counterfeiting and Piracy in the European Union, Europol, EUIPO 2017, available at: https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union

phishing' in which the sender of the mail passes off as the boss of an organisation and tricks an employee at the organisation into transfer money, internal documents or other types of assets to the sender[48].

An attacker will often have established a *spoofing website,* that is, a website that is a close imitation of the official website of the impersonated company or person, which is why a visit to the website does not create any suspicion about the malicious circumstances[49]. The phishing mail will often contain a hyperlink to the said website, but the website can also be visited independently. At the website, the victim will be prompted to reveal information such as 'updated' credit card information, 'confirmation' of passwords and similar sensitive information.

Depending on what the user is lured into doing, such acts may result in one or more criminal offences.

It is *fraud* if the attacker manages to lure the victim into paying a sum for a non-existing obligation or a non-existing product or service. If the attack results in installation of ransomware, it can be characterised as *extortion,* and installation of malware may amount to *vandalism*[50]*.*

Cybersquatting and other IPR infringing uses of domain names

Domain names play a key role in a number of the various types of IPR infringements in the online environment.

Cybersquatting was the first widespread type of IPR infringing use of domain names. Cybersquatting means registration and use of a domain name that is identical or confusingly similar to another's trade mark and where the registration and use is in bad faith and with the intention to somehow profit from the registration and use[51]. A variation of cybersquatting is *typosquatting* where a registrant acquires misspellings of other's domain names with the intention of catching and exploiting the traffic that was intended for the genuine websites. Both phenomena continue to take place in high numbers[52], which may be explained not only by the implementation of the many new generic top-level domains such as .xyz and .top, but also by the continuous development of ways to gain revenue from such registrations such as 'pay-per-click' revenues and revenues based on affiliate advertising schemes[53].

[47] Definition from Business Model study.

[48] See, inter alia, 'CEO Phishing Scams Up the Identity Theft Stakes' at: http://www.idtheftcenter.org/

[49] See Canvas 16 in 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016.

[50] The terms fraud, extortion and vandalism are used in their generic sense, and not as legal definitions of specific crimes.

[51] There does not seem to be a uniform definition of the term. The term stems from the US Anticybersquatting Consumer Protection Act (ACPA), 15 USC §1125(D) but is used in many other contexts and with different meanings.

[52] 'WIPO Cybersquatting Cases Hit New Record in 2017' at: http://www.wipo.int/pressroom/en/articles/2018/article_0001.html

[53] See the description of such revenue schemes in paragraph 5.3.2 in 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016.

The DNS is, however, being used for other types of infringing use of others trade marks. The abovementioned cases of fraudulent email *phishing scams* and *spoofing websites* do thus most often make use of domain names that include the trade mark of the imitated brand owner[54].

[54] See the business models involving use of others' trade marks in domain names described in Canvasses 3, 4, 5, 16, 17 and 19 ibid. of 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016. Reference is also made to the examples of recent case-law in Knud Wallberg: Recent Developments in Domain Name Law and Practice under the .dk Top-Level Domain, NIR 1, 2017, p. 40 ff. (www.nir.nu).

7. THE LEGAL LANDSCAPE: AN OVERVIEW OF THE EXISTING LEGISLATIVE MEASURES CAPABLE OF BEING USED TO COMBAT AND PREVENT ONLINE IPR INFRINGEMENTS

7.1 EU level

The EU has adopted a number of legislative instruments that are capable of being used to combat and prevent online IPR infringements.

The harmonised IPR legislation [55]

The IPR legislation sets out the conditions for *how* protection for intellectual property rights can be acquired and the scope of the *exclusive rights* to exploit the protected creations. The exclusive character of IPRs implies that the rights holders can prevent others from exploiting the protected creations without the holders' permission and that the rights holders can combat occurring infringements through the court system, for example, by obtaining a legal injunction against the suspected infringer.

> The registration of a trade mark shall confer on the proprietor exclusive rights therein
>
> Article 10(1) of the TMDIR

> Member States shall provide for authors, in respect of the original of their works or of copies thereof, the exclusive right to authorise or prohibit any form of distribution to the public by sale or otherwise
>
> Article 4(1) of the InfoSoc Directive

Most of the provisions in the harmonised IPR legislation are 'technology neutral', meaning that the provisions apply regardless of which technological means are used to produce the protected creations or which means are used for an infringing activity. This is, for example, true for the provisions in the EU Trade Mark Regulation and Directive. Article 9 of the EUTMR, that defines the scope of the trade mark owners exclusive right, thus uses the term 'using in the course of trade', which is a term that not only

[55] Reference is made to the definition of IPR in Chapter 5.

applies to affixing the infringing sign to goods or their physical packaging but also to the use of an infringing sign as domain name [56] or AdWord [57].

This holds true also for a number of provisions in the InfoSoc Directive [58]. However, this Directive also contains provisions that are 'technology dependent' in the sense that they only apply to certain technology-specific situations, such as Article 5(1) that exempts certain temporary acts of reproduction whose sole purpose is to 'enable a transmission in a network between third parties by an intermediary' from the general reproduction right in Article 2.

The InfoSoc Directive also differs from the other substantive IPR legislation by containing a specific provision targeted against intermediaries, namely Article 8(3):

> Article 8(3). Member States shall ensure that rights holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

The Directive on enforcement of IPRs

In addition to the abovementioned instruments, the EU has adopted the Directive on enforcement of intellectual property rights (IPRED) [59], which harmonises the *civil enforcement measures and remedies* that will be available to IPR holders in the event of infringements. IPRED requires all Member States to provide for such measures, procedures and remedies that are necessary to ensure the enforcement of intellectual property rights, cf. Article 1. The provisions of the IPRED are technology neutral and do apply to enforcement if IPRs in the online environment. In this context, the 'increasing use of the internet [that] enables pirated products to be distributed instantly around the globe', was mentioned as an important reason for adopting the IPRED [60]. The IPRED contains provisions on:

- obtaining and preserving of evidence;
- right of information on the origin and distribution network of the infringing goods and services;
- provisional and precautionary measures such as interlocutory injunction and seizure or delivery up of the goods suspected of infringing an intellectual property right;

[56] EU:C:2013:516, Case C-657/11, BEST v Visys.

[57] EU:C:2010:159, Case C-236/08 et al., Google v Louis Vuitton.

[58] 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.

[59] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30 April 2004).

[60] See Recital 9.

- measures resulting from a decision on the merits of the case such as corrective measures, and injunctions;
- damages and legal costs;
- publicity measures such as publication of the judicial decision in part or in full.

Therefore, IPRED does address some of the issues that are included in this study. However, since IPRED sets up the minimum rules, it allows the Member States to provide for legal means that are more favourable to rights holders than the measures, procedures and remedies mentioned in IPRED[61]. In addition, the provisions of IPRED that are relevant in this context, are worded in general terms such as 'Member States shall ensure that, ...', which implies that there is a leeway for each Member State on how to implement the provisions of IPRED.

The purpose of this study is not to analyse and evaluate the application and effectiveness of the relevant provisions of the IPRED as such, which is a work that has recently been concluded by the European Commission[62]. Rather, the study will focus on whether and to what extent the current legal framework provides the rights holders or the enforcement authorities with legislative measures that can be applied in relation to the eight specific topics, which have been identified as being of particular interest in this context. Reference is made to these eight topics in Chapter 8 of the study.

The Directive on electronic commerce

The Directive on electronic commerce[63] is also of major importance in regards to online enforcement of IPRs. The Directive conditions the limitations of the liability of internet intermediaries in general, which includes their prospective liability in cases where their services are used for IPR infringing activities. In that context the Directive operates with three categories of intermediary services, namely 'mere conduit', 'caching' and 'hosting'. The Directive is based on the principle that the intermediaries are not obliged to monitor the information, which they send or store, nor do they have general obligation to actively seek facts or circumstances indicating illegal activity[64]. However, if an intermediary has obtained knowledge or has become aware of such illegal activities the intermediary is required to act expeditiously to remove or to disable access to the information if it is to stay within the 'safe harbour' provisions of the Directive.

[61] As explicitly stated in Article 2.1.

[62] DG GROW. See 'COMMISSION STAFF WORKING DOCUMENT, SWD (2017) 431 final' available at: https://ec.europa.eu/docsroom/documents/26601

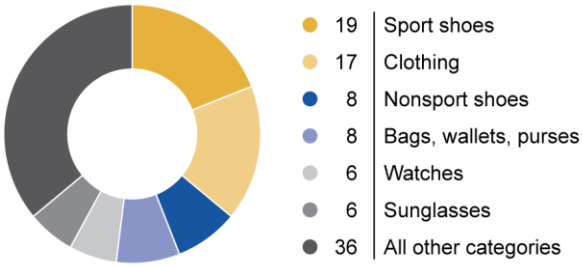
[63] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17 July 2000).

[64] Article 15 and Recital 47.

The Regulation on customs enforcement of IPRs

The Regulation on customs enforcement of IPRs (customs regulation)[65] provides the procedural rules for customs authorities to enforce intellectual property rights in relation to goods that are liable to customs supervision or customs control on the EU outer border. If such goods are suspected of infringing an IPR, the release of the goods may be suspended and the goods may be detained by customs authorities at the border if the requirements laid down in the regulation have been met.

FIGURE 2 — CUSTOM SEIZURES TOP CATEGORIES BY PROCEDURES[66]



The customs regulation is applicable to goods that have been acquired and have been shipped from a location outside of the EU to a customer within the EU, regardless of whether the purchase was completed online or otherwise.

> In the Blomqvist v Rolex case the CJEU stated that the customs regulation also applies to situations where counterfeited goods are sold to a person residing in an EU Member State through an online sales website in a non-member country.
>
> Case C-98/13, EU:C:2014:55

[65] Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003 (OJ L 181, 29 June 2013).

[66] Figures from the latest 'REPORT ON EU CUSTOMS ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS — RESULTS AT THE EU BORDER 2016'.

The European Investigation Order and the European Arrest Warrant

There are no specific European legal instruments targeting administrative or criminal enforcement of IPRs, but the European Investigation Order (EIO) (under implementation)[67][68] and the European Arrest Warrant (EAW)[69] can be used to some extent in relation to the enforcement of IPRs including online infringements.

The EIO covers any investigative measure including:

- temporary transfer of persons in custody in order to gather evidence;
- checks on the bank accounts/finances of suspects;
- covert investigations and intercepting telecommunications;
- measures to preserve evidence.

The EIO enables judicial authorities in one EU Member State (the issuing state) to request that evidence be gathered and transferred from another EU Member State (the executing state). The EIO is based on the mutual recognition so each EU Member State[70] is in principle obliged to recognise and carry out such a request, which must be made swiftly and without any further formality. For example, police in one Member State could ask their counterparts in another Member State to conduct house searches or interview witnesses on their behalf[71].

The EAW is a simplified cross-border procedure for prosecuting or executing a custodial sentence or detention order. An EAW is a request issued by a judicial authority in one Member State to detain a person located in another Member State and to surrender the said person for prosecution in the requesting Member State. 'Counterfeiting and piracy of products' as well as 'computer related crimes' are included in the list of offences, which do not require that the offence is also a criminal act in the executing state.. This is a derogation from the otherwise existing requirement of 'double criminality', meaning that the offence that forms the background for the EAW is punishable in both the issuing state and in the executing state. The EAW implies that the Member States cannot refuse to surrender, to another EU

[67] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the EIO in criminal matters (OJ L 130, 1 May 2014).

[68] And its predecessor the European Evidence Warrant; Council Framework Decision 2008/978 of 18 December 2008 on the European evidence warrant for obtaining objects, documents and data for use in proceedings in criminal matters (OJ L 350, 30 December 2008).

[69] Council Framework Decision 2002/584 of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18 July 2002).

[70] Except Denmark and Ireland.

[71] The example is the one mentioned at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:230301_2

Member State, their own citizens who have committed a serious crime or are suspected of having committed such a crime in another Member State on the grounds that they are nationals.

The Directive on the prevention of money laundering

The purpose of the Directive on the prevention of money laundering [72] and the financing of terrorism is to prevent that the financial market and its institutions are being misused for this purpose by:

- facilitating the work of the designated authorities of each Member State to identify and follow suspicious transfers of money and facilitate the exchange of information;
- establishing a coherent policy towards non-EU countries that have deficient anti-money laundering regimes;
- ensuring full traceability of the transfers of funds within, to and from the European Union.

The legal instruments within this area are largely based on international standards [73] and are further complemented by national rules in the individual Member States.

7.2 International level

The TRIPS Agreement

On the international level, the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) [74] provides for internationally harmonised minimum standards for the protection and enforcement of IPRs. The sections that address enforcement measures contain provisions on:

- obtaining of evidence and information on the infringement and the infringer (Article 47);
- application of preliminary measures such as preliminary injunctions (Article 50);
- suspension of release of infringing goods by the customs authorities (Article 51);
- criminal procedures and penalties (Article 61).

[72] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for money laundering and terrorist financing (OJ L 309, 25 November 2005) and Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5 June 2015).

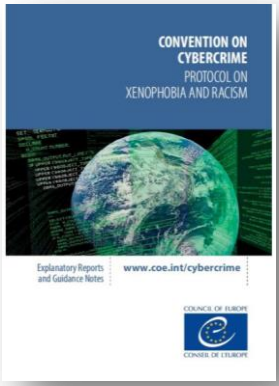
[73] Adopted by the Financial Action Task Force at: http://www.fatf-gafi.org/home/

[74] Agreement on Trade-Related Aspects of Intellectual Property Rights. The TRIPS Agreement is Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on 15 April 1994. The EU as well as all of the Member States are party to this Agreement.

The Cybercrime Convention

In addition, the Cybercrime Convention [75] has established a number of instruments that can be of relevance to the enforcement of IPRs in the online environment, in particular in cases that involve signatory states that are not Member States of the EU [76]. The convention explicitly covers offences related to infringements of copyright and related rights [77]. The Cybercrime Convention does not contain specific provisions on trade marks. However, provisions on computer related forgery and fraud [78] could indirectly encompass the misuse of third-party trade marks in phishing scams.

FIGURE 3



7.3 National level

This study is based on the premise that the EU Member States have implemented and apply the abovementioned EU legal instruments in their national legislation. As regards the international legal instruments, it is assumed that implementation has been made in regard to ratified legal instruments. It is acknowledged, however, that not every EU Member State has ratified all international legal instruments in this area (for example, the Cybercrime Convention), and some Member States may have done so under reservation.

Since these measures do not include, and therefore do not fully harmonise all the legislative measures that may be applied to combat IPR infringements, the individual Member States may and very often have adopted, implemented and applied specific national legislative measures either generally addressing enforcement of all types of rights or more specifically designed to enforce IPR infringements.

As regards *civil measures*, the study shows that these measures include, but are not limited to:

- regulations for registration and use of the country code top-level domain (whether legislative measures such as the applicable provisions in the Belgian Code of Economic Law and the

[75] Council of Europe, Convention on Cybercrime, CETS 185, Budapest 23 November 2001, at: https://www.coe.int/en/web/cybercrime/home. The convention entered into force on 1 July 2004 and is ratified by all EU Member States.

[76] The Convention on Cybercrime has been signed and ratified by 56 countries, and signed but not yet ratified by four countries. Ratifying countries include all EU MS, except Ireland and Sweden. See: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=0Uu2kbyk (Accessed 18 January 2018).

[77] See Article 10.

[78] Articles 7 and 8, Convention on Cybercrime, COE (ETS No 185).

Croatian regulation on the .cr TLD, or measures based on the terms and conditions of the Registry, such as in the UK and in Poland);

- application of the rules of unfair competition and the general principles of tort law on IPR infringements (such as in the Netherlands, Italy, Germany, Denmark et al.);
- regulations establishing notice and take-down procedures (such as in Greece and Italy).

As regards *administrative measures*, the study shows that these include, but are not limited to:

- establishment of administrative bodies dedicated to pursuing IPR infringements (such as the Intellectual Property Commission in Spain);
- establishment of Alternative Dispute Resolution (ADR) bodies dealing with conflicts of domain name registrations (which applies in most Member States)[79].

On *criminal measures*, 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.

The rules on when an IPR infringement may be subject to criminal sanctions and who is entitled to initiate criminal proceedings vary from Member State to Member State.

The starting point of a criminal procedure may be that the concerned rights holder files a complaint to the relevant public enforcement authority, but the authorities may also initiate *ex officio* investigations and criminal proceedings independently of the IPR holder. This is the case when an infringement is classified in the law as a public crime in which case the prosecutor's office or another enforcement authority has, by law, a duty to initiate a criminal investigation and subsequently has the authority to decide on whether or not to initiate criminal prosecution. Typical examples include, but are not limited to:

- situations where the institution of proceedings is required in the interests of the public (Denmark, Germany);
- infringements on a commercial scale (Bulgaria, Germany, Greece);
- infringements that include money laundering (Belgium, Luxembourg);
- infringements where the infringer obtains a substantial or unlawful gain (Croatia, Denmark);
- infringements that cause substantial damage (Croatia, Hungary, Slovakia);
- infringements that take place under aggravating circumstances (Greece, Italy, Lithuania et al.);
- infringements carried out by organised criminal groups (Belgium, Bulgaria, France et al.).

[79] ADRs are available in all Member States except in the Czech Republic, Germany, Lithuania, Luxembourg, Malta and Slovakia.

Both the minimum and the maximum penalties possible for IPR infringements vary considerably. Often the maximum penalties prescribed by national law depend on a pre-classification of severity of the criminal act. In this sense, infringements may be subsumed to different types of crime ('ordinary infringement' v 'counterfeit or piracy') and mitigated or aggravated depending on the infringing conduct (negligent or with intent) and the scope of infringement (large scale, commercial scale, organised crime, committed as part of a list of serious criminal offences, or to finance terrorism, etc.)[80]. The penalties may be included in the specific IP legislation or in the penal codes. It is also common that the infringement is classified as a specific type of criminal offence in IP legislation, but the concrete penalties are described in the penal code. Either way, general provisions of the penal law and penal procedure law will in most cases be applicable to IPR infringements.

In addition, *other provisions* in the penal codes may also apply to IPR infringements such as general provisions on fraud and forgery. Where IPRs are being considered as equivalent to other property rights even theft and vandalism may apply. Specific provisions on electronic communications fraud and other financial crimes may also be applicable, in situations where the purpose of the IPR infringement is to obtain sensitive data or direct financial gain. Interpol calls such infringements 'social engineering frauds' and it covers situations where IPR protected products are pretended to be offered for sale but no product is actually sent to the consumer. The unauthorised offer of IPR protected goods or services are only made to induce consumers to purchase goods that are never received or to reveal personal data.

7.4 Mapping of the legislative bases for the analysed legislative measures in the EU Member States

The illustration below provides an immediate overview of the legislative bases for those civil legislative measures that will be looked into in this study. The most notable observations are:

In relation to Topic 1 on measures for obtaining account information and Topic 2 on measures that allows for the blocking of access to websites, legislation in the Member States does not only consist of provisions that reflect the relevant provisions of the IPRED. In most Member States the implemented provisions of the IPRED are thus complemented by specific, that is, non-harmonised national legislation, and in some cases such specific national provisions are listed as being the legal basis for obtaining account information and blocking of access to websites[81].

[80] These expressions and others have emerged in our mapping exercise as English translations to classifications of IPR infringements. The translations received are not official.

[81] EU is applied where only one or more of the IPRED boxes have been ticked in the questionnaire; NAT is applied where only the box on national measures (i.e. national legislation that is not a result of the implementation of the IPRED) has been ticked; both is applied where the box on national measures has been ticked in addition to one or more of the IPRED boxes; n/a (not answered) is ticked by the respondents where the matter is listed as unresolved and in some cases where the answer is no.

FIGURE 4 — OBTAINING ACCOUNT INFORMATION

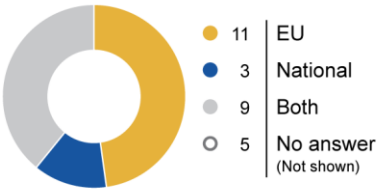
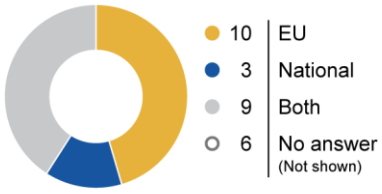


FIGURE 5 — BLOCKING ACCESS TO WEBSITES



As regards Topic 3 on domain name actions, the picture is notably different, since the legal basis for the deletion, suspension or transfer of domain names is exclusively found in national legislation and/or in the policy for registration of domain names that each ccTLD Registry has laid down.

FIGURE 6 — DOMAIN NAME ACTIONS, REGISTRY

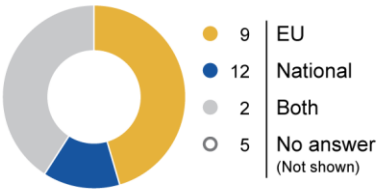


FIGURE 7 — DOMAIN NAME ACTIONS, REGISTRAR

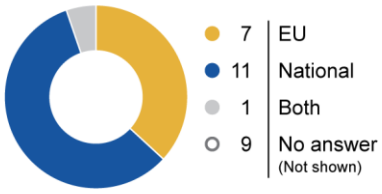
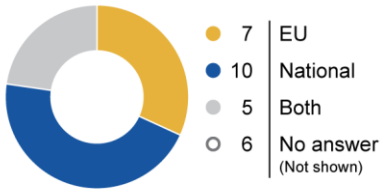


FIGURE 8 — DOMAIN NAME ACTIONS, REGISTRANT



The answers to Topic 4 on actions targeted at hosts reveal a fragmented picture of the legal basis. The most notable difference lies in the uncertainty about the availability of a legal basis for the suspension of future accounts.

FIGURE 9 — TAKEDOWN OF INFRINGING MATERIAL

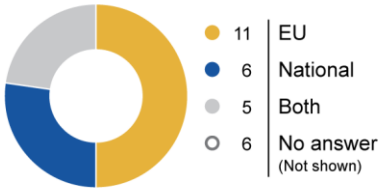


FIGURE 10 — SUSPENSION OF EXISTING ACCOUNTS

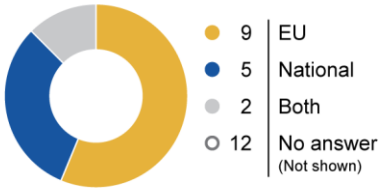
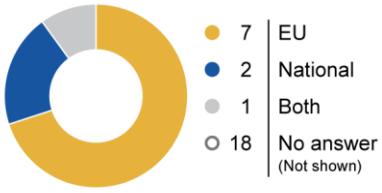


FIGURE 11 — SUPENSION OF FUTURE ACCOUNTS



Criminal law is not harmonised by EU law, and consequently, the criminal measures that are available in the Member States are based on national legislation and their implementation of the international treaties in particular the TRIPS Agreement and the Council of Europe Cybercrime Convention. Despite such progress in harmonisation, national traditions still dictate considerable divergence, in particular as regards actual maximum penalties.

As far as the judicial cooperation between the EU Member States in criminal matters is concerned, there are, however, a number of measures that are available to the relevant authorities in cross-border cases. These measures include investigative and evidence preservation measures, arrest and extradition and money laundering.

Whether these differences in the legal basis do or do not lead to differences in the actual availability and application of the specific legislative measures that are the subjects of this study will be demonstrated in the following chapter.

8. ANALYSIS OF SELECTED, HORIZONTAL TOPICS

8.1 Introduction

Production, marketing, distribution and sale of illicit goods such as pirated software or counterfeited brands are per definition unlawful acts. The applicable IP legislation thus provides the proprietor with the exclusive right to the original products, just as the legislation includes various civil and criminal remedies that the proprietor can rely on to pursue infringements of these rights. Traditionally, the proprietor will pursue IPR infringements through the court system or the administrative system, and such actions are initiated against the suspected infringer that may be the producer, the distributor or the vendor of the IPR infringing goods.

It is however, widely recognised that such actions often fall short when it comes to effectively combat infringing actions in the online environment and the rights holders as well as relevant enforcement authorities have looked for other ways to pursue IPR infringements in the cross-border digital environment. This development has led to a situation where the various online intermediaries have become the 'natural points of control' when it comes to enforcement[82].

The study will reflect this, and will thus include analyses of whether and to what extent the existing legislative measures may be used and be employed both in relation to the immediately suspected infringer and in relation to the relevant intermediaries.

The project team identified the following eight horizontal issues that should be the focus of the horizontal analyses of the study.

[82] On p. 9 in Perel (Filmar), Maayan and Elkin-Koren, Niva, Accountability in Algorithmic Copyright Enforcement (21 February 2016). Stanford Technology Law Review, Forthcoming. Available at: SSRN: https://ssrn.com/abstract=2607910 or http://dx.doi.org/10.2139/ssrn.2607910 it is put in the following way: 'Online intermediaries have acquired an important role in managing online behaviour and enforcing the rights of internet users. They offer a natural point of control for monitoring, filtering, blocking and disabling access to content, which makes them ideal partners for performing civil and criminal enforcement.'

TOPIC	KEYWORDS
1. Obtaining account Information	Retrieval of information from online intermediaries on: • the account holder contact information (the challenge of false contact information); • the IP addresses that are used for the infringing actions; • WHOIS information related to the domain name.
2. Blocking of access to websites	Websites hosted in the Member State itself. Websites hosted in other EU Member States. Websites hosted in non-EU Member States.
3. Domain name actions	Types of actions (suspension, transfer, etc.) towards: • the Registry • the Registrar • the Registrant.
4. Actions targeted at hosts	Actors hosting or advertising infringing material: • takedowns of concrete listings; • suspension, blocking etc. of specific vendor accounts; • suspension, blocking etc. of future accounts of a specific account holder.
5. European Investigation Order	Its application to online infringements of IPR, and if so its application to: • requesting information on bank accounts; • freezing or confiscation of the deposits of such accounts; • locating and seizing servers used for suspected infringements; • interception and seizing of counterfeited products before they reach the consumer.
6. Extradition — European Arrest Warrant	Its application to online infringements of IPR, and if so its application to: • extradition of infringers or suspected infringers from other EU Member States.
7. Money laundering	Its application to online infringements of IPR.
8. Criminal sanctions	Maximum sentences. Time limits for prosecution. Infringements on a non-commercial scale. Objective liability. Liability for companies.

For all eight topics, it was envisaged that there would be challenging jurisdictional issues related to all of the topics, and that it was best to include these issues continually in the analyses of the eight topics.

It was further envisaged that Topic Nos 5-8 would mostly be dealt with from a descriptive approach systematising the pertinent legislative measures, whereas Topic Nos 1-4 would require a more analytical approach.

8.2 Obtaining information on the identity of the suspected infringer

Introduction

Once it has been evidenced that an IPR infringement takes place, the next step in an enforcement action is to establish the identity of the suspected infringer. Usually, to initiate an enforcement action it is a precondition for a rights holder or for the investigator or prosecutor to establish who the infringing party is, where the party is located and how to contact the party.

This task to establish the identity and contact details of the suspected infringer is often faced with challenges when it comes to IPR infringements in the online environment, since the identity of the suspected infringer is not immediately available.

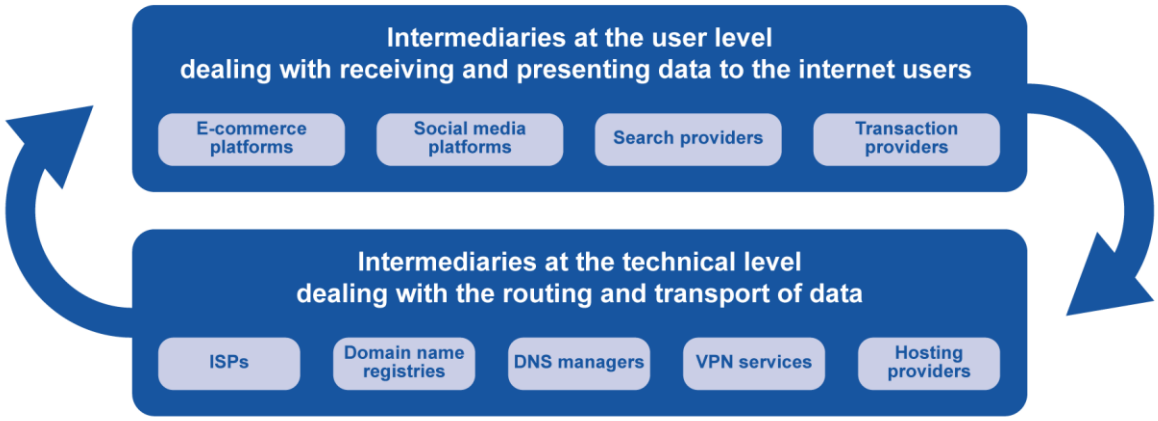
In the event of streaming copyright protected material such as live music or sports events, and sharing files with copyrighted works such as films and music, it is often possible to determine the IP address[83] that has been used for the infringing activities.

However, further investigative actions are required to establish the legal identity of the entity that used the particular IP address in the execution of an IPR infringement. Additionally, an alleged infringer might conceal its IP address by technical means or use a third party IP address.

If the infringing activity takes place on an online platform of a third party, such as an online market place or a social media platform, it may be possible to identify the 'account' of the alleged infringer. While the specific identification of the holder of the account is not immediately available to third parties such information is privy to the operator of the marketplace or social media platform.

[83] See the definition above in Chapter 5.

FIGURE 12 — EXAMPLES OF ONLINE INTERMEDIARIES[84]



Likewise, if the infringement occurs on a dedicated website, that is, a website that uses a specific domain name as its internet address.

Websites that are used to promote or to distribute products or services that are suspected of infringing the IPR of a third party do seldom — if ever — contain true and reliable information on the party controlling the website, neither in the form of an imprint nor in the form of other contact information. Domain registries will maintain a publicly available WHOIS database of the registrants, but the correctness of the information in these databases does to a large extent depend on the correctness of the information that is provided by the registrants — and this is not always true and correct[85]. Additionally, in certain top-level domains, registrants of a domain name can rely on the use of a privacy or proxy service, which conceals the identity of the real registrant in the WHOIS register.

[84] The figure only includes those types of intermediaries that are considered to be relevant in this context. There are several other types of intermediaries than the ones that are mentioned here, just as there are other ways to divide and name them than the one that is applied.

[85] The issue of false contact information is mentioned several times in the WIPO Overview of WIPO Panel Views on Selected UDRP (Uniform Domain Name Dispute Resolution Policy) Questions, Third Edition, available at: <http://www.wipo.int/amc/en/domains/search/overview3.0/>. See as an illustrative example, Section 6B in WIPO Case DNL2017 'Dr. Martens' International Trading GmbH / 'Dr. Maertens Marketing GmbH v Olga Olga' on the domain name <doktermartens.nl>.

FIGURE 13 — REGISTRATION OF DOMAIN NAMES

It is therefore important — and in most cases even essential — to establish whether an online intermediary whose services are being used by one of their customers to carry out IPR infringing activities can be ordered to disclose information on the identity of the customer that they have in their possession.

Disclosure of the identity of the holder of a particular account

The rights holders' right to information in IPR infringement cases is stipulated in Article 8(1) of the IPRED. According to this provision the competent judicial authorities may order that the *infringer* — as well as any other person who is '*found to be providing on a commercial scale services used in infringing activities*' such as the various online intermediaries — will present information on the '*origin and distribution networks*' of the infringing goods or services.

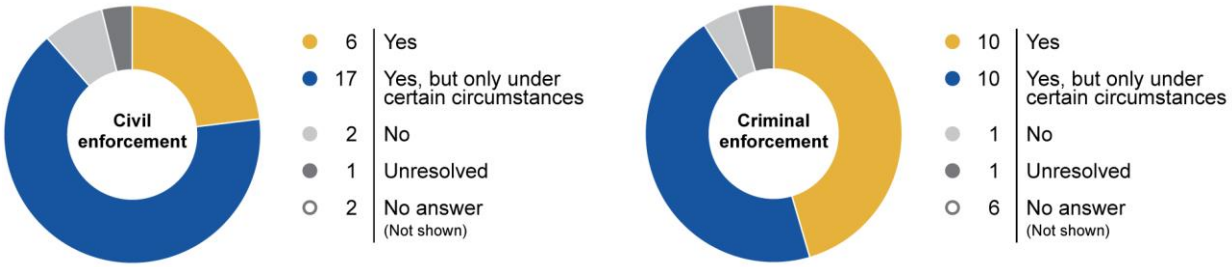
The provision does thus not specifically address the right to obtain 'account information', but being a minimum Directive the IPRED does allow Member States to implement provisions, which grant rights holders 'rights to receive further information'[86].

The mapping of the national legislative measures shows that the legislation in all Member States (except Malta and Slovenia) can *in general* be applied by the competent judicial authority[87] to order an internet intermediary to disclose such account information, if the request meets the general procedural requirements of being 'justified and proportionate'[88].

[87] Usually the courts. In Spain the Intellectual Property Commission can also order the disclosure of such information. The prosecutor can also request such information in criminal proceedings.

[88] Or similar wording to that effect.

FIGURE 14 — DISCLOSURE OF THE IDENTITY OF AN ACCOUNT HOLDER

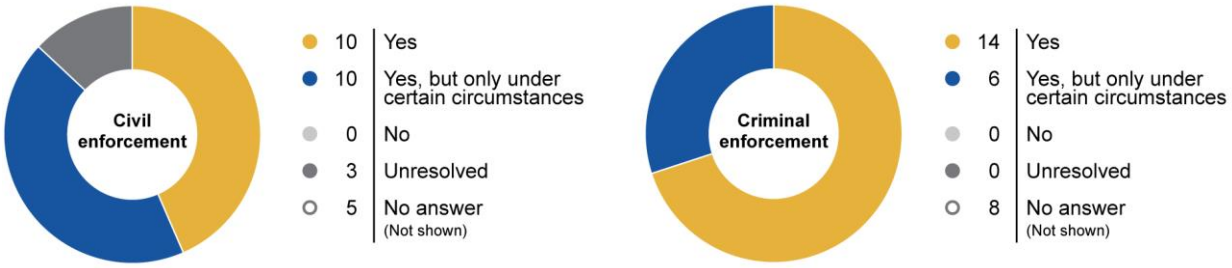


On criminal enforcement measures, the mapping of the national legislative measures shows that almost in all EU Member States an online intermediary can be asked to disclose account information on a particular customer, with the exception of Germany where such is reported as not being possible and Spain, where the matter is unresolved. Procedure requirements may apply, such as the measure being requested by a competent authority[89] and authorised or validated by a judicial authority[90], and that the order fulfils general requisites and procedural guarantees.

Contact information on the holder of a specific account

In relation to *contact information on the holder of a specific account* on the online network or platform such as a social media network or a digital marketplace, the mapping demonstrates that it is possible in civil procedures to get a judicial decision that orders the provider of the online service to disclose this information.

FIGURE 15 — DISCLOSURE OF THE CONTACT INFORMATION OF AN ACCOUNT HOLDER



[89] Public prosecutor, police or administrative enforcing agency.

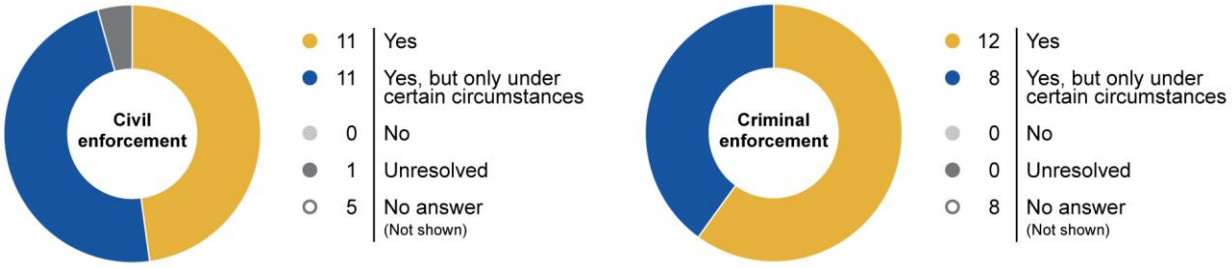
[90] Depending on the jurisdiction, a court order may be necessary. Otherwise, the public prosecutor may be able to directly order or request such information.

In criminal proceedings, the mapping shows that in all Member States that allow the possibility of ordering an intermediary to disclose account information on specific costumers, such will entail the possibility to obtain individual contact information of the account holder.

Contact information on persons or entities using an IP address for IPR infringing activities

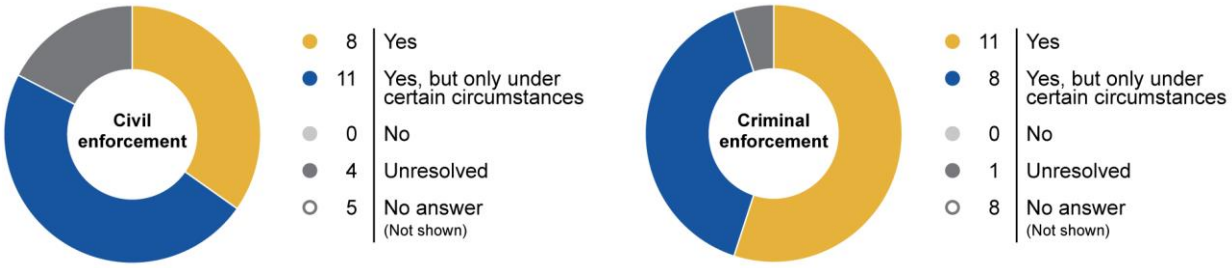
As regards the *contact information on a person or an entity that uses an IP address* or makes a server available under an IP address provided by its access provider, the overall picture is the same as for the abovementioned account information: it is possible in all Member States to get a judicial decision that orders the provider of the online service to disclose this information.

FIGURE 16 — DISCLOSURE OF THE CONTACT INFORMATION OF THE USER OF AN IP ADDRESS



In terms of criminal measures aimed at procuring *contact information of a person or an entity that uses an IP address* or makes a server available under an IP address provided by its access provider, the situation is similar. All Member States that allow the possibility of ordering an intermediary to disclose account information on specific costumers will also allow authorities to order that information on the person using an IP address and making a server available under an IP address (with the exception of Greece and Spain, where this issue is reported as being unresolved or debatable) is to be disclosed.

FIGURE 17 — DISCLOSURE OF THE CONTACT INFORMATION OF THE PROVIDER OF THE SERVER



IP addresses and associated information can be personal data in the sense of the General Data Protection Regulation, which means that the rules and principles of the Directive must be observed in these cases. This is the case for static IP addresses, as well as for dynamic IP addresses.

The third category of accounts that has been addressed is the contact information of the registrant of a domain name.

If the registrant of a domain name is an individual person, the registrant may possibly [91] invoke the applicable rules on the protection of personal data in which case the registrant can request that registrant information [92] will not be publicly accessible in the WHOIS database. In addition, some registries allow the registrants to use privacy services or proxy holders, in which the identity of the 'real' registrant is concealed behind the name of the proxy.

In all such cases, it is therefore important to establish whether it is possible to obtain a court decision that orders the relevant registry to disclose the information on the 'real' registrant.

The mapping of the empirical evidence in this study shows that such information can, in principle [93],be ordered to be disclosed to the requesting party in all Members States [94], even though the procedures that must be followed to obtain such information varies.

In the corresponding criminal enforcement measures mapping, almost all Member States have answered that if an online intermediary can be asked to disclose information on a particular user/client, such possibility includes the issuance of an order to disclose information on the 'real' contact information of the registrant of a domain name (if the registrant is anonymous or uses a privacy service or the like in the publicly available WHOIS).

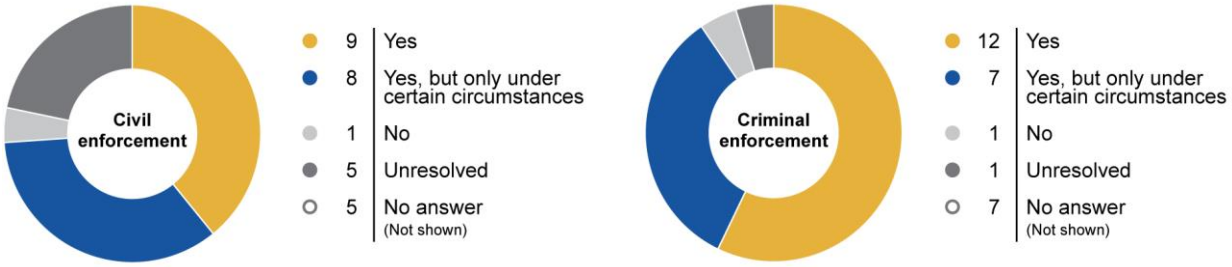
[91] The issue is not settled yet at EU level.

[92] Which usually include name, address, telephone number and email address.

[93] The matter is listed as unresolved in six Member States.

[94] Which is also the case for the .eu TLD. See https://eurid.eu/en/register-a-eu-domain/domain-name-disputes/

FIGURE 18 — DISCLOSURE OF THE TRUE IDENTITY OF THE REGISTRANT OF A DOMAIN NAME



8.3 Blocking of access to websites

Introduction

If an IPR infringing activity takes place on or through a dedicated website it is immediately evident that it will be an effective way to disrupt the current activities and to prevent them from taking place in the future if the access to the website by the internet users in general is blocked [95].

Blocking orders have, therefore, become an import legal remedy that is frequently used [96] by both rights holders and by prosecutors [97].

Another reason for the effectiveness and popularity of this measure is that the defendants in these cases are the various intermediaries that provide the technical access to the internet to their customers, often referred to as access providers [98]. These providers are regularly established companies that can be immediately identified, and thus be the subjects of legal actions.

[95] See below in Section 8.4 on inactivation of a website by targeting the website's domain name and Section 8.5 on measures targeted at the hosts of the infringing activities.

[96] Statistics/reference to mapping exercise.

[97] See, inter alia, the reoccurring Europol operation 'In Our Sites' at: https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-in-our-sites-ios-vi

[98] https://dictionary.cambridge.org/dictionary/english/access-provider

> *Online intermediaries have acquired an important role in managing online behavior and enforcing the rights of Internet users. They offer a natural point of control for monitoring, filtering, blocking, and disabling access to content, which makes them ideal partners for performing civil and criminal enforcement.*

Quote 99

Blocking of the access to a website is, however, a limited and targeted legal measure. The website as such will thus still exist and may be accessible for those internet users, whose access provider is not covered by the blocking order, including providers in other jurisdictions than the one in which the blocking order is issued.

An access provider that is not the direct subject to a blocking order may, however, voluntarily agree to follow such an order. It is thus noteworthy that major providers in a number of Member States have agreed to implement blocking orders against a specific website or a specific service even if the blocking formally is only aimed at one of the providers that are part of the agreement [100].

In most Member States, the courts are the only competent authority to grant blocking orders. In Italy a blocking order may however also be issued by the Italian Competition Authority (AGCM). In Slovakia, the .sk domain name registry SK-NIC can block access to an .sk domain name that is used for illegal activities, not only based on a court order but also at its own discretion.

The general rule on the exemption of the liability of access providers in civil matters [101] is set out in Article 12(1) of the E-commerce Directive, and implies that the access provider is not liable for the information that is sent by its customers, if certain, specified conditions are met. This 'safe harbour' provision does not, however, affect the possibility for the courts or the administrative authorities of the

[99] Quote from p. 9 in Perel Filmar, Maayan and Elkin-Koren, Niva: Accountability in Algorithmic Copyright Enforcement (21 February 2016). Stanford Technology Law Review, Forthcoming. Available at: SSRN: https://ssrn.com/abstract=2607910 or http://dx.doi.org/10.2139/ssrn.2607910

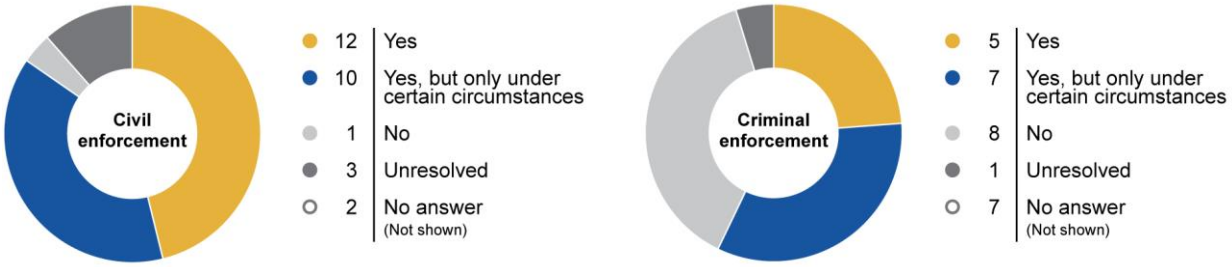
[100] Some illustrative examples are the 2015 Portuguese Memorando de Entendiemento (Memorandum of Understanding) which is published in Portuguese at: https://paulasimoesblog.files.wordpress.com/2015/09/memorando.pdf, and the 'Code of Conduct for handling decisions to block access to services which infringe intellectual property rights' adopted by the members of the Telecom Industry Association — Denmark, http://rettighedsalliancen.dk/wp-content/uploads/2017/04/CoCrev_dec16_UK.pdf

[101] The issue of liability in criminal matters are not subject to harmonisation at EU level.

Member States to require that access providers terminate or prevent infringements, in accordance with each Member States' legal systems [102]. It follows from Article 11, third sentence of the IPRED [103] and Article 8(3) of the InfoSoc Directive, that Member States will ensure that rights holders are in a position to apply for an injunction against intermediaries whose services are used by third parties to infringe IPRs, such as when a website contains copyright infringing material or us used to offer counterfeited goods.

Injunctions in the form of blocking orders are therefore a remedy, which are in principle available in all Member States [104] except Slovenia [105], and in both civil and criminal proceedings [106].

FIGURE 19 — BLOCKING OF ACCESS TO WEBSITES



It is common ground that a blocking order can only be issued if it is found to be both an effective and proportionate remedy in the specific case [107]. Apart from this, both the substantive and the procedural requirements that must be met in order for a court to issue a blocking order varies from Member State to Member State [108]. The following are illustrative examples of such differences.

In some Member States, the legal bases are the general rules on preliminary injunctions, such as in Denmark where the legal basis is Section 413 in the Administration of Justice Act.

[102] Cf. Article 12(3) of the E-commerce Directive.

[103] Directive 2004/48: Directive on the enforcement of intellectual property rights.

[104] In Bulgaria, Cyprus and Poland the matter is reported as 'unresolved'.

[105] Blocking orders have been issued in relation to illegal online gambling websites.

[106] Hungary reports that the remedy is only available in criminal proceedings.

[107] The two said criteria are explicitly stated in Article 3(2) of the IPRED.

[108] As pointed out above in Section 7.1, the IPRED is a minimum Directive. Furthermore, the relevant provisions are worded in rather broad terms. It follows from general EU law that each Member State decides how to implement directives. Further, there is no harmonisation of the rules on civil and criminal procedures at EU level.

In other Member States, the provisions on blocking of websites that infringe copyright are found in the Copyright Act, such as in Finland and in the UK [109].

In Austria and Germany, it is a prerequisite for initiating a court action that the rights holder beforehand has made reasonable efforts to get the ISP (internet service provider) to block the access to the website(s) in question, for example, by way of a cease and desist letter.

As regards the issue that is inextricably linked to online infringements, namely the issue of territoriality, the courts of a Member State only have jurisdiction over matters that are related to or have an effect on the territory of the said Member State. Blocking orders can therefore as a starting point only be issued if the activities on the website at issue infringes or may infringe IPRs that are protected in the said Member State.

Where this may be the case has been touched upon by the Court of Justice of the European Union (CJEU) in paragraphs 64 and 65 of Case C-324/09, L'Oreal v eBay [110]. In the judgment the CJEU stated that the mere fact that a website is accessible from a territory that is covered by [an IPR] [111] is not a sufficient basis for concluding that the offers for sale displayed at the website are targeted at consumers in that territory. Rather, it falls to the national courts 'to assess on a case-by-case basis whether there are any relevant factors on the basis of which it may be concluded that an offer for sale, displayed on an online marketplace accessible from the territory that is covered by the [IPR], is targeted at consumers in that territory'. The CJEU only mentioned one such relevant factor, namely that if the sales offer is accompanied by details of the geographic areas to which the seller is willing to dispatch the product that information is of particular importance.

In other words, it is yet not established in detail at the EU level when such infringements may occur. The respondents to the questionnaire were therefore asked to address whether the competent authorities can issue a blocking order, in which access is blocked to websites hosted in the Member State itself, hosted in another Member State or hosted in non-EU Member States.

[109] In the UK, the requirements for obtaining a blocking order in cases of trade mark infringements is enunciated in the Cartier International v British Sky Broadcasting decision (EWCH.Ch.2003.3354).

[110] EU:C:2011:474. In the decision, the CJEU refers to the joined Cases C-585/08 and C-144/09 *Pammer and Hotel Alpenhof*, [2010] ECR I-12527, paragraph 69.

[111] The case concerned trade marks.

FIGURE 20 — BLOCKING ORDERS FOR WEBSITES HOSTED IN THE EU MEMBER STATE ITSELF

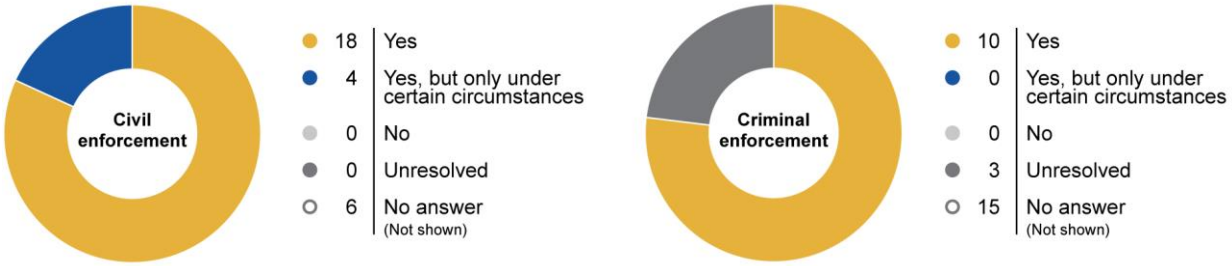


FIGURE 21 — BLOCKING ORDERS FOR WEBSITES HOSTED IN OTHER EU MEMBER STATES

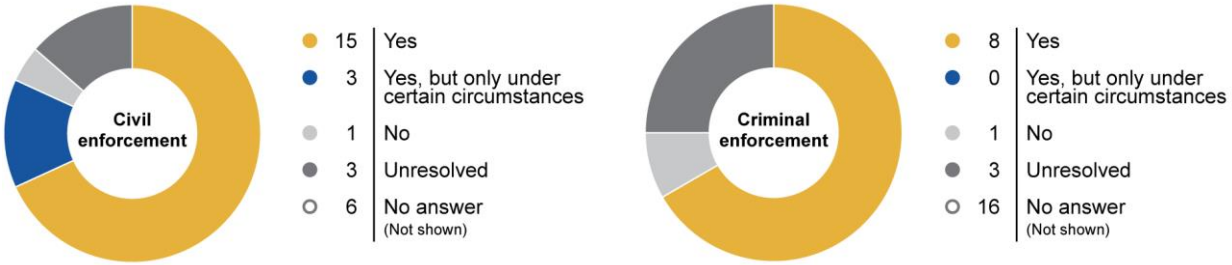
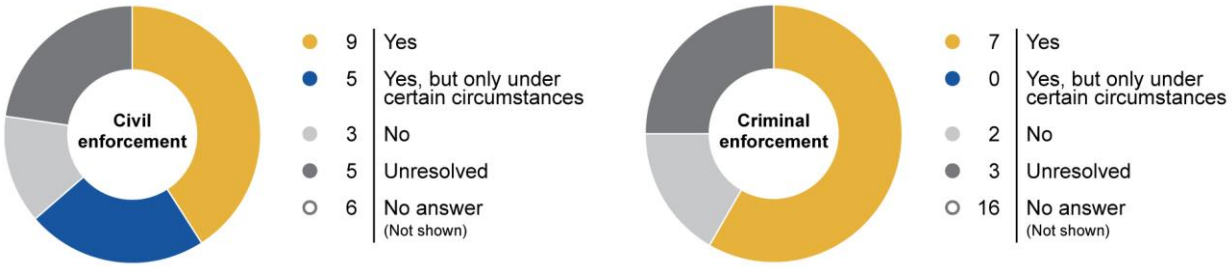


FIGURE 22 — BLOCKING ORDERS FOR WEBSITES HOSTED IN NON-EU MEMBER STATES



8.4 Domain name actions[112]

Introduction

As mentioned above in Chapter 6, domain names play a key role in a number of the various types of IPR infringements in the online environment, and have done so for two decades. The well-known phenomenon of cybersquatting continues to take place[113], while at the same time the registrants are continuously finding new ways of monetising on the registrations of such cybersquatted domain names such as through bulk registrations of expired domain names that are then used either to set up what pretends to be web shops or to host websites with advertisements or commercial links that are generated through the affiliate advertising[114].

The DNS is also being used for other types of unauthorised uses of trade marks such as in fraudulent email phishing scams, and for spoofing websites that install malware or ransomware on the unsuspecting internet users' computers or portable devices when they are visited[115].

FIGURE 23 — FICTITIOUS PHISHING EMAILS

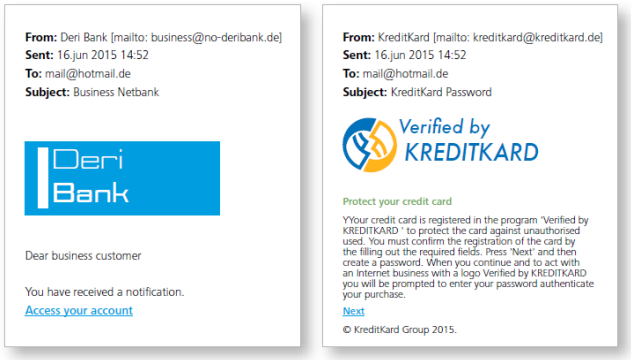


Illustration of phishing emails from 'Research on Online Business Models Infringing IPRs', EUIPO, 2016.

[112] Given the overall purpose of the study, this section is restricted to only include analysis of the ccTLDs of the Member States as well as of the .eu TLD.

[113] 'WIPO Cybersquatting Cases reach New Record in 2017', at: http://www.wipo.int/pressroom/en/articles/2018/article_0001.html .

[114] See 'Research on Online Business Models Infringing Intellectual Property Rights — Phase 2 Suspected trade mark infringing e-shops utilising previously used domain names', EUIPO 2017.

[115] See the business models described in Canvasses 3, 4, 5, 16, 17 and 19 in 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016.

Domain names are also used as internet addresses for websites that are used for various copyright infringing activities, such as websites with links to illegal digital content, websites that contribute to video streaming and torrent websites[116]. In these situations it is not the domain name per se that is infringing but the content of the website.

Partly as a consequence of the comprehensive harmonisation within the EU of the laws on copyrights and neighbouring rights and on trade marks, the legal situation is clarified on some important points. If a domain name is used for IPR infringing activities, a court may order the infringer to *cease* the infringing activities under the domain name, just as the court may impose damages, fines and other sanctions, whether civil, criminal or both.

It is, however, important to establish whether there are additional legislative measures that can be applied to *prevent* that the infringing use of a domain name is resumed. The study, therefore, focuses on whether the following legislative measures on domain names are available in EU Member States, and to what extent these measures can be applied towards the registrants, the registrars and the registries respectively[117]: suspension, deletion, transfer and seizure.

At the outset, the DNS is not governed by any international treaty[118], nor are the country code top-level domains (ccTLD) that are specific for each EU Member State subject to harmonisation at the EU level. Consequently, the specific requirements for the registration, transfer etc. of domain names under the ccTLDs may vary from Member State to Member State, and, as it will be demonstrated in the following paragraphs, there are also differences as to which legislative measures can be applied if a domain name is used for IPR infringing activities.

A civil or criminal action that involves use of a domain name will, as a starting point, be the *registrant* of the domain name, since it is justified to presume that the registrant on record is also the entity that is responsible for the actual use of the domain name[119].

However, it is important to consider whether the legislative measures apply to the other key players of the DNS, primarily the ccTLD registries, and the registrars in their capacity as 'name server managers' (NSMs).

Suspension of domain names

The suspension of domain names means the inactivation of the name servers assigned to a disputed domain name**.**

[116] See the business models described in Canvasses 21, 22, 23 and 25 in 'Research on Online Business Models Infringing Intellectual Property Rights', EUIPO, 2016.

[117] Reference is made to the description of the role of these actors in the description of the domain name system above in Chapter 5.

[118] See the explanation of the domain name system above in Chapter 4.

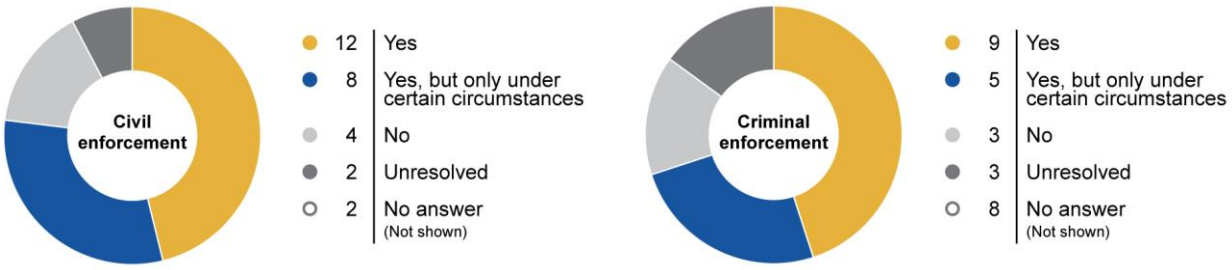
[119] This is, however, not always the case. See above in Section 8.2.4 on anonymous or concealed registrants.

When a domain name is registered, it is a requirement that the domain name is assigned to at least two active domain name servers. The assignment of these domain name servers is also a prerequisite for the domain name to function, whether as a website address or as address for emails[120]. The DNS servers may be operated by the registrar of the domain name but they may also be operated by an independent access provider often referred to as a 'name server manager' (NSM). It is the registrant that choses the provider of the DNS service and the registrant may at any time change the provider. To act as an NSM for a particular ccTLD, the NSM has to be accredited by the ccTLD registry.

The fact that the DNS servers are vital for the functioning of a domain name also means that it is possible to disrupt ongoing infringements and to prevent future infringements if it is possible to 'cut off' the connection between the domain name and the assigned name servers.

Such 'inactivation' of the assigned name servers can — technically speaking — take place both at the registry level and at the NSM level. In this context the issue that is addressed is whether the relevant ccTLD registry can be ordered to 'suspend' or 'inactivate' a domain name that is suspected to be used for IPR infringing activities[121]. This is indeed possible in most of the ccTLDs of the Member States as well as for the .eu TLD, but the specific requirements that must be met to obtain the suspension of a domain name varies from Member State to Member State. The replies from Bulgaria, Cyprus, Ireland, Poland and Sweden indicate that the issue is presently unresolved and appears not to be possible in Austria and Hungary.

FIGURE 24 — SUSPENSION OF DOMAIN NAMES BY THE ccTLD REGISTRY



Transfer of domain names

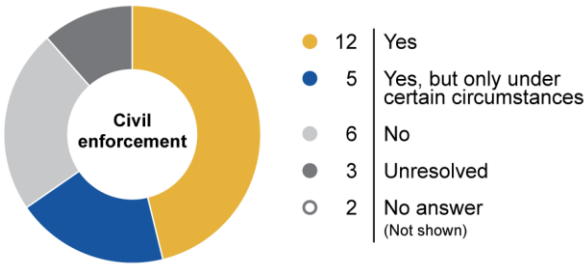
The registrant of a domain name may, as regards all the ccTLDs and the .eu TLD, voluntarily assign the domain name to another registrant, provided the new registrant also meets the criteria for being recorded as registrant under the specific ccTLD registry.

[120] Reference is made to the detailed explanation of the domain name system above in Chapter 5.

[121] The NSMs are assumed to be covered by the definition of an 'intermediary service provider' in the E-Commerce Directive, in which case they are subject to the liability exemption rules in Section 4 of the Directive. An analysis of these issues appears in Torsten Bettinger and Allegra Waddell (ed.): 'Domain Name Law and Practice. An International Handbook', 2nd edition, in Chapter XVI, p. 436 ff., which concerns the .de ccTLD and is written by Torsten Bettinger.

The issue that will be addressed in this context is whether a court or another dispute resolution body[122] can order the transfer of a disputed domain name from the present registrant to a new registrant. This is possible in most of the ccTLDs of the Member States, with the notable exceptions of Austria, Croatia, the Czech Republic, Finland, Germany and Hungary. Transfer is also available for .eu domain names.

FIGURE 25 — TRANSFER OF DISPUTED DOMAIN NAMES



Once the court or the dispute resolution body has made a final decision to transfer a domain name, the decision will be implemented by the registry of the concerned ccTLD once it has received notification of the enforceable decision[123].

In Austria, the Czech Republic and Hungary an infringing domain name registration can be cancelled after which it is released and the domain name can then be registered by the claimant, but it is not possible to obtain a court order to transfer a domain name directly from one registrant to another. Such a direct transfer is also not possible in Germany. As regards Austria, the Supreme Court has thus stipulated that Austrian law does not provide a legal basis for claiming a transfer of a domain name[124]. In the Czech Republic, the Czech Supreme Court has reached the same conclusion[125].

Deletion or cancellation of domain name registrations

The plaintiff in a civil dispute as well as the prosecutors in criminal disputes against a registrant of a domain name may not be interested in obtaining ownership of the disputed domain name. The question then arises whether deletion or cancellation of the disputed domain name are available remedies instead of transfer.

[122] Administrative dispute resolution bodies for domain names have been established in all ccTLDs and the .eu except for the .cz, .de, .lt, .lu, .mt and the .sk TLDs.

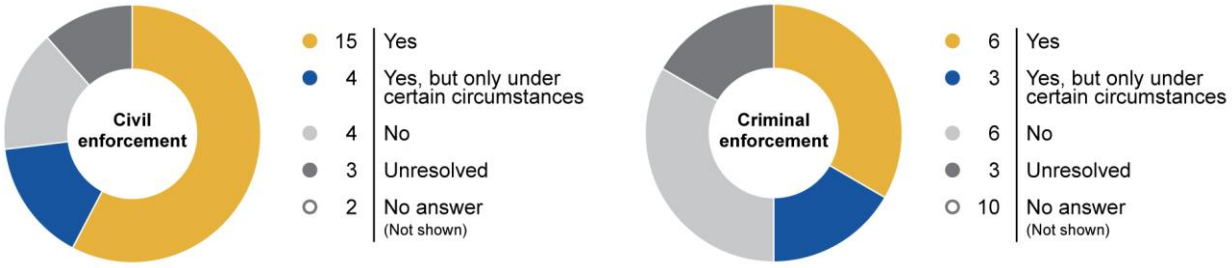
[123] This was confirmed by the answers to Question 3.1.1.

[124] In Case ZIR 2014/1 74 ff. of 22 October 2013.

[125] In Case 23 Cd 3407/2010 of 19 April 2012.

The overall picture is the same as it was for transfers, namely that the registration of a disputed domain name may be cancelled or deleted in respect of the ccTLDs of most of Member States, with the exception of Croatia, Finland, Germany and Sweden[126].

FIGURE 26 — DELETION OF DOMAIN NAME REGISTRATIONS



Seizure of domain names[127]

Within the last few years, the law enforcement authorities in a number of Member States have obtained court orders in which a large number of domain names have been seized. Most notably is the 'Operation In Our Sites' that is coordinated by Europol[128] and which has seized more than 4 500 domain names that were used as internet addresses for websites that were illegally selling counterfeit products to consumers online. These seizures took place in 27 different countries including 16 EU Member States[129]. One of the actors in the operation was the UK Police Intellectual Property Crime Unit (PIPCU). PIPCU, which was established in 2013, is a specialist police unit dedicated to protecting UK industries from intellectual property crime. The Danish Public Prosecutor continuously receives notifications from rights holders on .dk domain names that are used for such sites, and these are bundled and taken to the courts with an application to seize these specific domain names. A further example is that EURid, who is the registry manager of the .eu and .ею (Cyrillic script) country code top-level domains and Europol have signed a Memorandum of Understanding in which they undertake to join efforts in relation to combat cybercrime.

The legal basis that is applied to seize domain names is typically the general provisions on forfeiture. Since a domain name is not a physical commodity one can take along or lock up, the seizure entails that it is made sure that the disputed domain names are not transferred, deleted or otherwise released as

[126] Deletion or cancellation is also possible under the .eu TLD.

[127] Seizure of domain names was included as Question 9.1 in the questionnaire on criminal measures, as one example of 'property' that may be seized. The replies to this question are, therefore, not useable in this specific context.

[128] https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-in-our-sites-ios

[129] Austria, Belgium, Croatia, Denmark, France, Greece, Hungary, Italy, Lithuania, Luxembourg, Netherlands, Portugal, Romania, Spain, Sweden and the United Kingdom.

long as the seizure is in force. This can be secured in different ways such as by 'locking' the domain name, or by transferring the ownership of the domain names to the prosecutor, as it is done in Denmark.

8.5 Actions targeted at hosts

As mentioned above in Section 8.3, the various online intermediaries have become the 'natural point of control' when it comes to enforcement[130]. This is in particular so for those intermediaries that act as hosts, that is, the companies that operate the online platforms from or on which IPR infringing activities take place. Examples of hosts are digital marketplaces[131] and social media platforms[132].

The general rule on exemption of liability of hosting providers is set out in Article 14(1) of the E-commerce Directive, and the provision implies that the provider is not liable for the information that is stored by their customers, if the specified conditions are met. This so-called safe harbour provision does, however, not affect the possibility for the courts or the administrative authorities of the Member States of requiring hosting providers to terminate or prevent infringements, in accordance with each Member States' national legal systems[133].

The study has mapped and analysed three different types of legislative measures, namely, takedowns of IPR infringing sales offers or advertisements; blocking or suspension of existing accounts that are being used to disseminate or distribute infringing goods and services; and the possibility to block or otherwise prevent that suspected infringers can open future accounts.

'Takedowns' of infringing sales offers or advertisements for infringing goods

A 'takedown' is at the outset a procedure whereby a third party can file a complaint ('a notice') to an operator of an online marketplace, a social media platform or a similar platform and request the operator of the platform to remove ('take down') a product that is offered for sale or advertised on the marketplace

[130] On p. 9 in Perel (Filmar), Maayan and Elkin-Koren, Niva, Accountability in Algorithmic Copyright Enforcement (21 February 2016). Stanford Technology Law Review, Forthcoming. Available at: SSRN: https://ssrn.com/abstract=2607910 or http://dx.doi.org/10.2139/ssrn.2607910 it is put in the following way: 'Online intermediaries have acquired an important role in managing online behaviour and enforcing the rights of internet users. They offer a natural point of control for monitoring, filtering, blocking and disabling access to content, which makes them ideal partners for performing civil and criminal enforcement.'

[131] See Canvas 8 Marketing Goods or Digital Content on Third Party Online Wholesale Marketplace (B2B) in 'Research on Online Business Models Infringing Intellectual Property Rights. Phase 1 Establishing an overview of online business models infringing intellectual property rights', EUIPO, July 2016.

[132] See Canvas 9, Sale of Non-Genuine Goods through Social Media Networks, in 'Research on Online Business Models Infringing Intellectual Property Rights. Phase 1 Establishing an overview of online business models infringing intellectual property rights', EUIPO, July 2016.

[133] Cf. Article 14(3) of the E-commerce Directive.

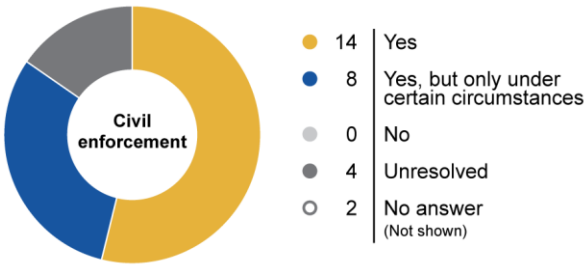
by a third party. It is then the individual operator of the platform concerned that decides whether to accept or to reject the complaint, that is, whether to take down the infringing listing or not[134].

Such 'notice and takedown' (NTD) procedures are implemented and applied by most digital marketplaces[135] as well as by most social media platforms and they form an integrated part of the platforms' terms and conditions. NTD procedures are used in huge numbers daily[136] and are generally perceived as efficient tools when it comes to enforcement if IPRs in the digital environment[137].

The issue that will be addressed here is, however, whether the operator of a digital platform can be ordered by a court or other dispute resolution body to take down such sales offers or advertisements[138].

The replies indicate that the remedy is in principle available in all Member States, although the issue has not been finally settled in all Member States[139].

FIGURE 27 — TAKEDOWN OF IPR INFRINGING LISTINGS ON ONLINE PLATFORMS



[134] See a very similar definition in paragraph 5 of the 2016 Memorandum of Understanding on the Online Sale of Counterfeit Goods, at: http://ec.europa.eu/DocsRoom/documents/18023

[135] Knud Wallberg: 'Notice and takedown of counterfeit goods in the Digital Single Market: a balancing of fundamental rights', Journal of Intellectual Property Law & Practice, Volume 12, Issue 11, 1 November 2017, pages 922-936.

[136] According to the statistical information that is available via the Lumen database at: https://lumendatabase.org/ (previously https://www.chillingeffects.org/), which is a project of the Berkman Klein Centre for internet & society at Harvard University. See also the annual Google transparency reports at: https://www.google.com/transparencyreport/?authuser=1 and the figures provided by the Alibaba Group at http://www.alizila.com/wp-content/uploads/2016/10/P-Alibaba-Group-Comments-for-2016-Notorious-Markets-Report-2_FINAL_compressed.pdf?x95431.

[137] 'A Digital Single Market Strategy for Europe', Communication from the European Commission, 6 May 2015, COM(2015) 192 final, Section 3.3.2., p. 12; 'Communication on Online Platforms and the Digital Single Market' {COM(2016) 288}, Section 5.II), p. 7 ff.

[138] In its judgment of 12 July 2011 in Case C-324/09, *L'Oréal* v *eBay*, the CJEU addressed a number of issues in relation to intermediaries acting as hosts. The Court did not specifically address the issue of takedowns.

[139] The answer to the question in the questionnaire was listed as unresolved in the following four Member States: Bulgaria, Cyprus, Poland and Romania.

That the measure is available 'in principle' means that, as it was stressed in a number of the replies, that it is a precondition for obtaining a takedown order against an operator of a digital platform that the specific requirements of the applicable law are met.

LISTING OF CIRCUMSTANCES
Finland: Court order is requested by the prosecutor, a person in charge of inquiries or a rights holder.
France: The court can order the suspected infringer or intermediary any measure to prevent imminent infringements and to stop continued infringing acts taking into account the principle of proportionality.
Hungary: Upon objection, the service provider will restore the contested information.
Ireland: Only if the applicable requirements under Section 40 of the CRRA (Copyright and Related Rights Act) are met.
Portugal: Article 210-G is applicable also for the suspension of an actual infringement and also vis a vis an intermediary whose service is being used for the infringement.
Slovakia: Upon effectual court decision or successful ADR procedure.
Spain: Requires a court order in which the general requirements for obtaining precautionary measures are met.
Sweden: Requires a court order and that the intermediary is contributing to the infringement.
Germany: Refers in the 'yes' section to the principle of 'Störerhaftung' [liability for interference].

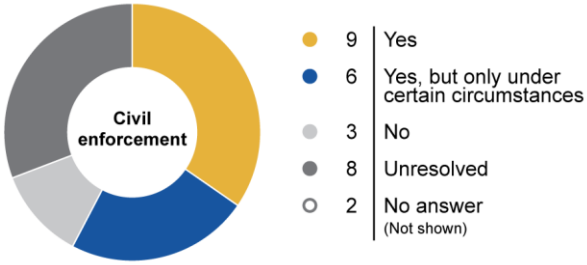
Suspension or blocking of existing accounts

In addition to the possible takedown of actual sales offers or advertisements, the issue often arises whether it is possible to get the 'account' that is being used for the infringing activities suspended or blocked. A suspension or blocking of an account will thus prevent the holder of the account to list new sales offers instead of the one(s) that have been taken down.

The question that was asked in this part of the study was whether an online intermediary, whose platform is being used to host the sale of or to advertise the sale of IPR infringing goods, can be ordered to suspend or block the account of the suspected infringer[140]. As it is shown below, the answers to this question revealed a quite diverse legal situation in the Member States.

[140] The user terms of a number of hosting providers contain provisions that allow the provider to suspend existing accounts for various reasons. One of the reasons frequently listed is (repeated) violation of the rules and policies on infringement of the IPRs of third parties.

FIGURE 28 — BLOCKING OR SUSPENSION OF EXISTING ACCOUNTS



Blocking or otherwise preventing the opening of future accounts by a specific vendor or advertiser

A vendor or advertiser whose account has been blocked or suspended can usually open up a new account with the same hosting provider immediately after the suspension of the previous account. The vendor or advertiser can then continue with its suspected infringing activities using the new account, until this account also is blocked and so on. This situation is, therefore, often referred to as the 'whack a mole' dilemma, and it is frequently highlighted as a major obstacle for effective, online enforcement[141].

In paragraph 144 of the judgment in Case C-324/09, L'Oreal v eBay, the CJEU stated that the third sentence of Article 11 of the IPRED must be interpreted as requiring the Member States to ensure that the national courts 'are able to order the operator of an online marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to *preventing further infringements* of that kind.' (italics added). However, the CJEU did not address whether the cited provision of the IPRED covers blocking of future accounts, so the issue is presently unresolved as regards this legal instrument.

Turning to the collected empirical data, the review shows that the present legal situation in the Member States may aptly be described as uncertain. It is possible to get a judicial decision that orders the involved intermediary to block the future accounts of an existing customer in eight Member States[142], while this is not possible in six Member States [143] and is unresolved in the remaining 12 responding Member States[144].

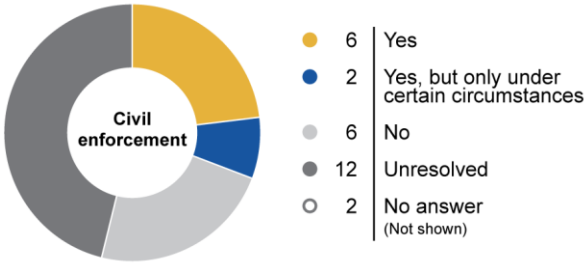
[141] See paragraph 21 in Frederick Mostert: 'STUDY ON APPROACHES TO ONLINE TRADE MARK INFRINGEMENTS', WIPO/ACE/12/9 REV. 2 available at: http://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_12/wipo_ace_12_9_rev_2.pdf

[142] Estonia, Germany, Ireland, Latvia, Malta, Portugal, Slovakia and the UK.

[143] Austria, Bulgaria, Hungary, Italy, Lithuania and Slovenia.

[144] That the present situation has been reported as being unresolved in 12 of the Member States does not mean that the measure is excluded from being applied. As it is put in the reply on the legal situation in France, it may well be possible to obtain such order if it is 'over a limited time, necessary and proportionate to its aim.'

FIGURE 29 — BLOCKING OR SUSPENSION OF FUTURE ACCOUNTS



8.6 European Investigation Order

Judicial cooperation between EU Member States in matters of criminal enforcement is growing. Online IPR infringements are not limited by national borders and the ability to obtain and preserve evidence in other EU Member States is a major concern and in many cases a pre-condition to the efficiency of enforcement measures. The EIO[145] is a legislative measure of judicial cooperation between Member States. It is based on mutual recognition of decisions, which means that each EU country is obliged to recognise and carry out the request of the other country, as it would do with a decision coming from its own authorities.

The EIO replaces previous fragmented legislative framework and creates one single comprehensive instrument with a large scope. It covers the whole process of collecting evidence, from the freezing of evidence to the transfer of existing evidence, for the participating Member States. The EIO has been created with strict deadlines for compliance with the request. Member States have 30 days to decide if they accept a request[146]. Once the request is accepted, the executing state has 90 days to conduct the requested investigative measure[147].

In particular, the EIO encompasses the following:

- temporary transfer of persons in custody in order to gather evidence (Articles 22 and 23);
- investigation of the bank accounts and financial operations of suspected or accused persons, including gathering of evidence in real time, continuously and over a certain period of time (Articles 26 to 28);
- covert investigations and intercepting telecommunications (Articles 29 to 31);
- measures to preserve evidence.

[145] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the European Investigation Order in criminal matters, *(EIO Dir.)*

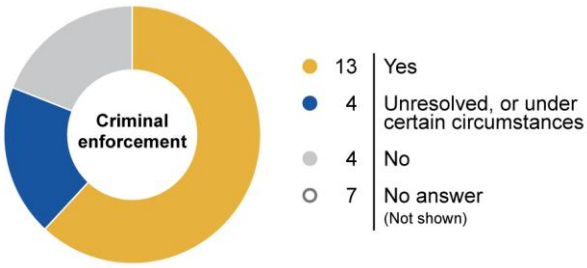
[146] Article 12(3) EIO Dir.

[147] Article 12(4) EIO Dir.

The receiving authority can only refuse to execute the order under certain circumstances, for example, if the request is against the receiving country's fundamental principles of law or harms national security interests. Article 11 contains a list of grounds for non-recognition or non-execution. These include situations where the EIO has been issued for conduct that does not constitute a criminal offence under the law of the executing state. The EIO Directive limits the applicability of such double criminality requirement by creating a list of offences which will always imply compliance if the issuing state punishes such conduct by a custodial sentence or a detention order for a maximum period of at least three years[148]. Counterfeiting and piracy of products are included in the list[149]. However, not every type of IPR infringement is considered to be 'counterfeiting and piracy', and not all Member States punish all types of infringement with custodial sentences with a maximum of at least three years. As it can be seen in Section 8.9 (Figure No 33) a significant number of Member States establishes as penalties for IPRs infringements either fines or less than three years of imprisonment.

A further ground for non-recognition or non-execution of relevance for enforcement of IPRs is the possibility that the specific investigative measure requested is restricted under the law of the executing state to certain types of criminal offences or to offences punished by a certain threshold. It may be the case that IPR infringement-related offences are punished[150].

FIGURE 30 — APPLICATION OF AN EIO ON ONLINE IPR INFRINGEMENTS



[148] Article 11(1)(g) EIO Dir.

[149] ANNEX D, EIO Dir.

[150] Article 11(1)(h) EIO Dir.

8.7 Extradition — European Arrest Warrant

Infringements of IPRs in the digital environment imply a delocalisation of infringer activities and infringers. Conducts may take place in several Member States simultaneously, while the alleged infringers may be located in one or several Member States. Judicial cooperation plays an important role in enforcement of IPRs in such cases.

The European Arrest Warrant (EAW)[151] is a simplified cross-border judicial surrender procedure for prosecuting or executing a custodial sentence or detention order. An EAW is a request issued by a judicial authority in one EU Member State to detain a person located in another Member State and to surrender them for prosecution. It can also be issued in order to execute a custodial sentence or detention order.

The EAW has been operational since 1 January 2004. It has replaced the lengthy extradition procedures that used to exist between EU countries. A warrant issued by one EU Member State judicial authority is valid in the entire territory of the EU. It operates through direct contact between judicial authorities and it is based on the principle of mutual recognition of judicial decisions.

An EAW can only be issued, prior to sentencing if an offence is punishable by imprisonment of at least 12 months, or in conviction cases, where the remaining term of imprisonment is four months or more[152]. As can be seen by FIGURES 35 and 36 this excludes a number of Member States concerning types of infringements considered less serious offences. Its use in IPR infringement cases is therefore limited.

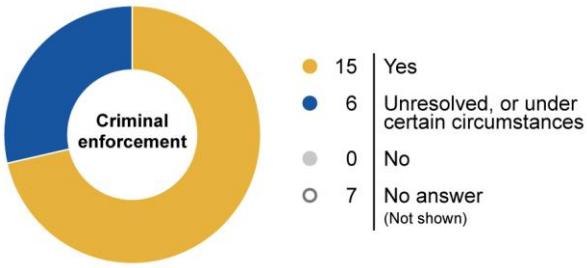
Under the EAW Framework Decision, the requirement for double criminality has been removed for a wide range of categories of crimes, if these are punishable in the issuing Member State by a custodial sentence or a detention order for a maximum period of at least three years[153]. 'Counterfeiting and piracy of products', as well as 'computer related crimes' are included on the list, however it is also required that the specific conduct of the suspected infringer is defined by the law of the issuing Member State as either 'counterfeiting or piracy of products' or 'computer related crimes'. As FIGURE 31 indicates a lack of harmonisation of the mentioned criteria in the Members States', it results that 'double criminality' seems to be the basic requirement in IPR infringement cases.

[151] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18 July 2002.

[152] Article 2(1).

[153] Article 2(2).

FIGURE 31 — 'DOUBLE CRIMINALITY' AS A REQUIREMENT IN CASES OF ONLINE IPR INFRINGEMENTS



In some jurisdictions it may be possible to argue that IPR infringing activities amount to organised crime expanding the applicability rules of the EAW. An example is the recent SweFilmer case[154], in which Swedish prosecutors linked illicit online streaming activities and underlying money laundering activities to organised crime and an EAW was applied when arresting and later extraditing one of the defendants from Germany to Sweden.

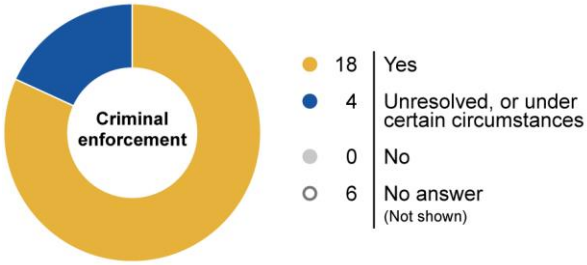
In almost every Member State an EAW can be issued or requested in connection with online infringement of IPRs. However, some respondents mentioned that this might not be possible in every case. According to Austrian law, infringements of IPRs will only be prosecuted upon request of the injured party[155]. The issuance of an EAW is therefore precluded[156]. Another example, in Romania, if the EAW is issued in view of conducting criminal prosecution or trial, it is only available if the offence committed corresponds to a maximum sentence of at least two years of imprisonment. As seen in FIGURES 35 and 36 maximum penalties for trade mark infringement range from three months to two years of imprisonment.

[154] Hovrätten for western Sweden Case No B 3143-17, decided on 18 March 2018. See also the 'DreamFilm' Case Linköping regional court Case No B 226-15, 9 May 2017 and Göta Appeal court, Case No B 1565-17, 22 February 2018.

[155] Section 91, paragraph 3 of the Austrian Copyright Law [Urheberrechtsgesetz]; Section 60a, paragraph 1 of the Austrian Trade and Service Marks Law [Markenschutzgesetz]; Section 35, paragraph 5 of the Austrian Design Law [Musterschutzgesetz].

[156] Section 71, paragraph 5, last sentence of the Austrian Code of Criminal Procedure.

FIGURE 32 — APPLICATION OF THE EAW ON ONLINE IPR INFRINGEMENTS IN GENERAL



Prior to the EAW several Member States national laws did not allow extradition of national citizens or permanent residents for the purposes of criminal prosecution. Under the Framework Decision, Member States are precluded from refusing the surrender of their own nationals wanted for the purposes of prosecution.

However, Article 4 establishes grounds for optional non-execution of the EAW. In cases where the infringing conduct is qualified as counterfeiting or piracy of products or as computer related crimes and the infringement is punishable with up to more than three years of prison in the issuing Member State, the executing judicial authority may refuse to execute the EAW if the act on which the EAW is based does not constitute an offence under their national law[157].

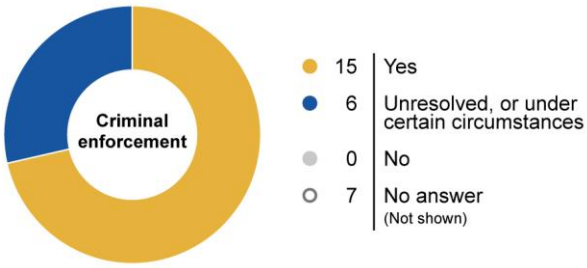
The same applies if the EAW has been issued for the purposes of execution of a custodial sentence or detention order, where the requested person is staying in, or is a national or a resident of the executing Member State and that state undertakes to execute the sentence or detention order in accordance with its domestic law[158].

Furthermore, under Article 5(3), executing Member States may subject the surrender to the condition that, after being heard, the person is returned to the executing Member State in order to serve the custodial sentence or detention order passed against the person in the issuing Member State.

[157] See Articles 4(1) and 2(4).

[158] Article 4(5).

FIGURE 33 — APPLICATION AF AN EAW IN RELATION TO NATIONAL CITIZENS OF THE EXECUTING STATE



EXAMPLES OF CIRCUMSTANCE WHERE EAWs MAY FACE REFUSAL OR BE SUBJECT TO CONDITIONS

Austria: In principle, the extradition of Austrian citizens due to an EAW is possible (Section 5, paragraph 1 EU-JZG). Extradition is not possible if the Austrian criminal laws apply to the offences committed (Section 5, paragraph 2 EU-JZG) or the offences have been committed in a non-EU country and there is no Austrian jurisdiction on them (Section 5, paragraph 3 EU-JZG). The extradition of Austrian citizens for the purpose of executing a custodial sentence or detention order is not permissible (Section 5, paragraph 4 EU-JZG).

Belgium: In principle, the extradition of Belgian citizens or permanent residents is possible. However, it may be refused under certain circumstances: 1. EAW for execution of sentence: refusal is possible if Belgium decided to undertake the execution of the sentence; 2. EAW for prosecution, can be subject to the condition that the surrender is returned to Belgium after being judged, in order to execute the sentence in Belgium (Articles 6 and 8 Belgian law on the EAW, 19 December 2003).

Finland: Extradition for execution of a custodial sentence will be refused if the requested person is a citizen of Finland and requests to serve the custodial sentence in Finland. In such case, the custodial sentence will be enforced in Finland. This is a ground for mandatory refusal under Finnish Law on EAW.

Italy: In principle, an EAW can be issued in respect to Italian citizens. However, there are limitations: 1) EAW for prosecution: extradition is subject to the condition that the person, after being heard, is returned to Italy to serve the custodial sentence or detention order (Article 19 lett. c L. 69/05); 2) EAW for execution of sentence will be refused, but the judicial authorities will order the execution of the sentence in Italy, according to applicable Italian law. This is a mandatory ground for refusal (Article 18 lett. r della L. 69/05).

Romania: The executing Romanian judicial authority may refuse to execute an EAW when it was issued for executing a custodial sentence or a custodial safety measure, if the requested person is a Romanian citizen and declares that she/he refuses to serve the sentence or the safety measure in the issuing Member State.

Slovenia: On EAW for execution of sentence of national citizens, EU citizens or permanent residents: It

may be refused if the requested person declares that he or she wishes to serve the sentence in the Republic of Slovenia, and if a national court undertakes to execute the sentence of the court of the ordering State in accordance with the national legislation, on condition that the circumstances exist which enable the execution of the sentence in the Republic of Slovenia.

8.8 Money laundering

Commercial scale IPR infringements are by definition all about earning money on the illegal activities. As it has been demonstrated and documented in many studies and reports the money involved in IPR infringing activities in general is huge. The latest figures covering the situation in the EU alone thus talk about an estimated value of counterfeited products that are imported in the EU — EUR 85 billion[159], and although precise figures are not available, it is presumed that a vast and growing part of these activities takes place online[160].

The 'follow the money' approach is regarded as an important means to prevent and combat these illicit activities, including IPR infringements. This approach does not only enable the authorities to identify, seize and confiscate the money but it also enables or at least facilitates to establish the identity of the perpetrators. Legislative measures tackling money laundering can be used indirectly as a tool to disrupt organised, large-scale activities that involve IPR infringements. Money laundering can be described as a process by which proceeds originating in illicit activities are converted into property such as assets or values with the purpose of hiding their provenance[161]. Money laundering is usually associated with types of organised crime that generate vast profits, such as trafficking in drugs, weapons and people, but the phenomenon does in principle cover proceeds originating from all types of fraudulent activities, which includes proceeds originating form IPR infringements.

The new anti-money laundering framework consists of two legal instruments (IP/15/5001): 'The Fourth Anti-Money Laundering Directive'[162] and 'The Fund Transfers Regulation'[163], both adopted on 20 May 2015.

[159] See the EUIPO/Europol publication: '2017 Situation Report on Counterfeiting and Piracy in the European Union' available at: https://euipo.europa.eu/ohimportal/da/web/observatory/observatory-publications

[160] See the Observatory publications on the economic cost of IPR infringements in various sectors. Reference is also made to the report Measuring IPR infringements in the internal market, 2012 that was prepared by RAND Europe for the European Commission, Internal Market and Services Directorate-General.

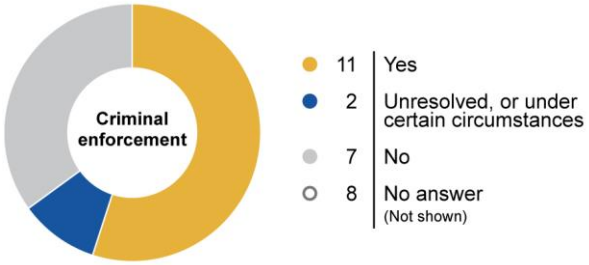
[161] For the definition in EU law, see Article 1(3) Money Laundering Dir.

[162] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (text with EEA relevance) OJ L 141, 5 June 2015, pages 73-117. (Money Laundering Dir.).

E-commerce and the use of new digital technologies provide both time-effective and cost-effective solutions to legitimate businesses and to customers as well as offering fertile ground for new and innovative forms of illicit activity and money laundering. As mentioned in Recital 18, the money laundering Directive will apply to the activities of the obliged entities [164], which they conduct on or via the internet. The Directive has been transposed by 20 Member States.

The Swedish case SweFilmer [165] illustrates this 'follow the money' investigative approach, and how anti-money laundering enforcement measures can be used in the enforcement of IPRs. In this case, involving streaming of unlicensed audio visual works, underlying money laundering activities were central to the investigation. The main defendant was charged both with copyright infringement and money laundering the profits of such illicit activity. The case ended on first instance with sentencing to both custodial penalty and payment of damages to the rights holders. Because money laundering carries higher penalties (six months to six years imprisonment) [166] than copyright infringement (fine or up to two years imprisonment) [167], the 'follow the money' approach was not only instrumental to unravelling the illicit activities and the persons responsible but also essential to the use of international cooperation investigative measures.

FIGURE 34 — APPLICATION OF PROVISIONS ON MONEY LAUNDERING TO ONLINE IPR INFRINGEMENTS



[163] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (text with EEA relevance) OJ L 141, 5 June 2015, pages 1-18.

[164] As defined in Article 2 of the Directive.

[165] Varberg Regional Court Case No T-1463-15 and Göta Appeal Court, Case No B 1565-17, 22 February 2018.

[166] 3§ Law (2014:307).

[167] 7 chp. 53§ Law (1960:729) (Copyright Law).

8.9 National criminal sanctions

Enforcement of IPRs against serious illicit conduct encompasses the availability of criminal sanctions capable of disrupting and preventing further infringements, both at a general level and in the specific case. This section examines the maximum sentence for online IPR infringements under the national legislation of each Member State. It was also surveyed (1) whether national law entails accessory or alternative penalties; (2) if national law punishes negligent infringements; (3) if infringements at a non-commercial scale are punishable; (4) whether Member States' national penal law entails objective criminal liability; and (5) if legal persons (including intermediaries) can be held criminally liable for online IPR infringements.

On the maximum penalties, the mapping exercise shows substantive differences between the Member States that provided data. Maximum possible imprisonment sentences range from two years to 10 years. In the vast majority of Member States surveyed, the penalties available are organised in a broad range, starting with the imposition of fines for less severe offences.

From previous studies and surveys, it is known that national definitions of counterfeiting and piracy, and the type of conduct typified as crimes vary considerably and are difficult to compare[168]. FIGURES 35 and 36 illustrate the maximum possible penalties. Maximum penalties are only considered in a limited number of cases where there are aggravated circumstances, such as commercial or large-scale infringements, organised crime or links to other criminal activities.

FIGURE 35 — MAXIMUM PENALTIES FOR TRADE MARK INFRINGEMENT[169]

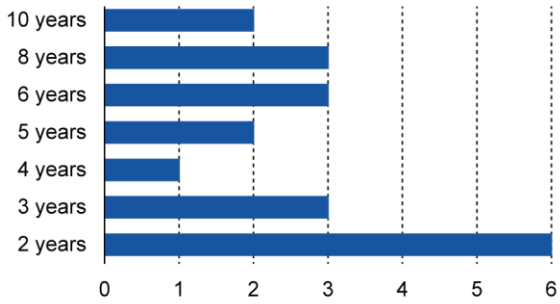
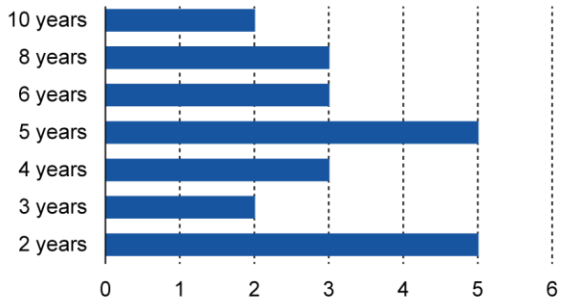


FIGURE 36 — MAXIMUM PENALTIES FOR COPYRIGHT INFRINGEMENT



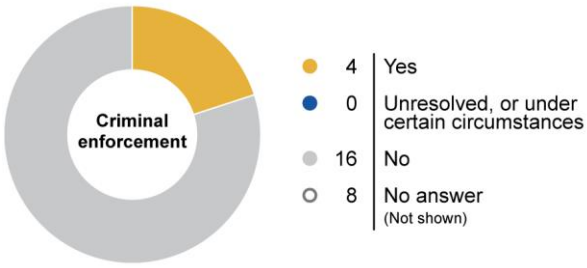
[168] INTA, 'Criminal Prosecution of counterfeiting and piracy in Member States of the European Union' (2010).

[169] The numbers on the x-axis in both figures refers to the number of Member States.

Accessory penalties or non-custodial sentences are possible in all Member States consulted. These appear under different titles and denominations and include for example: confiscation, forfeiture, seizure, destruction or removal from the channels of commerce of counterfeited and pirated goods; confiscation, forfeiture, seizure, destruction of objects or materials used in counterfeiting ad piracy of goods; publicity of the decision and public admission of guilt; liquidation (legal entities) and prohibition of future business (managers). The latter remedy was applied in the Spanish Bajatetodo case[170], in which the defendant was banned form creating or administering any website for a total of three years.

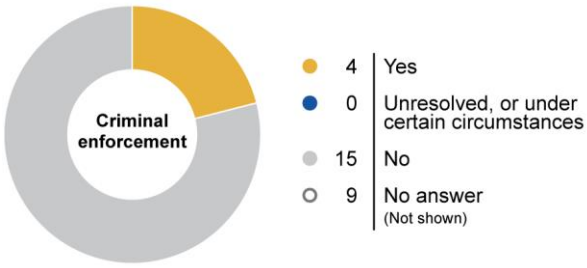
National criminal law requires a certain 'state of mind' or *mens rea* in order for an act of IPR infringement to be criminally sanctioned. National jurisdictions construct negligence and intent differently. Only a minority of Member States have reported that national law criminalises negligent[171] online conduct that constitutes IPR infringements.

FIGURE 37 — PUNISHMENT FOR NEGLIGENT IPR INFRINGEMENTS



In similarity, on objective or strict criminal liability for IPR infringements only four Member States reported that their national legislation allow IPR infringements to be punished in such circumstances.

FIGURE 38 — PUNISHMENT FOR OBJECTIVE IPR INFRINGEMENTS

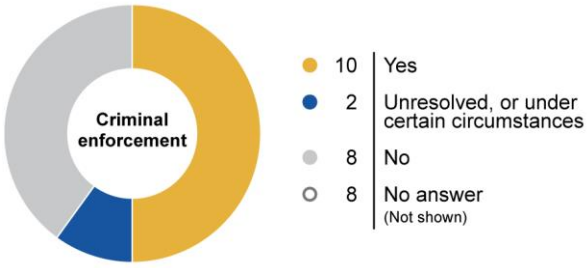


[170] Criminal Court of Appeal, Castellon, Resolution No 426/2014 of 12 November 2014.

[171] The laws in Germany and Denmark require 'gross negligence'.

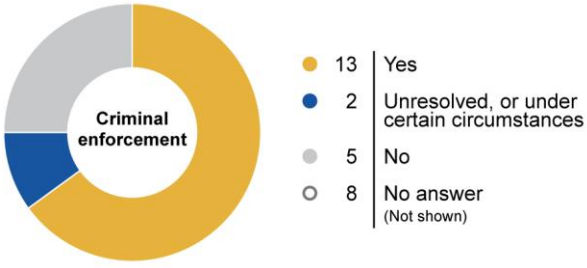
A considerable number of Member States exclude criminal liability if the infringement is not conducted on a commercial scale. The denomination 'commercial scale' is here used as an umbrella term to describe a variety of requirements found in national law such as: infringement in the course of trade, large-scale infringement, counterfeiting of a defined or undefined number of goods; committed in the course of trade or as a commercial activity, for profit. In such jurisdictions, small-scale counterfeiting and pirating limited to a small number of goods is not subject to criminal enforcement. Such may also entail that it is necessary to prove that the infringement has occurred at a certain scale or as part an economic activity.

FIGURE 39 — PUNISHMENT FOR IPR INFRIGEMENTS ON A NON-COMMERCIAL SCALE



Legal entities, in particular intermediaries, play an important role in the digital environment. Most of the respondents confirmed that legal persons can be criminally liable for IPR infringements. A number of accessory penalties and non-custodial penalties have been mentioned as applicable to IPR infringing entities. These include fines, foreclosure and prohibition of doing business.

FIGURE 40 — CRIMINAL LIABILITY FOR LEGAL ENTITIES IN RELATION TO ONLINE IPR INFRINGEMENTS



8.10 Some concluding observations

The main purpose of the study was to establish whether and to what extent a number of specific legislative measures, which can be applied to prevent or combat infringements of IPR in the online environment, are available in the Member States.

Further, the approach has been to focus on legislative measures that can be characterised as providing 'practical solutions to practical problems', which is why the study is primarily based on the replies from practitioners in the field to the two questionnaires.

While this approach is suitable to provide policy makers, civil society and private businesses with an overview of the current situations in the EU and its Member States, it does not give an in-depth insight into each individual topic. In order to gain such insight, further and more targeted studies will be necessary, and such studies seem to be particularly interesting for those topics where the analysis shows that the legal situation is either unresolved or is fragmented.

The above mapping and analysis of the *civil legislative measures* show both EU-wide commonalities and national differences.

In relation to the first two of the abovementioned eight topics, namely the legislative measures that concern the disclosure of information on a suspected infringer and the possibility to block access to websites, these measures are as a starting point available in all Member States. In most Member States, the harmonised legislation is however complemented by specific national legislation, such as the general laws on civil and criminal procedures, which means that the practical procedures differ from Member State to Member State

As regards the third topic on domain name actions, the picture is notably different. The EU has not harmonised national legislation on registration and administration of the country code top-level domains (ccTLDs) of the individual Member States. This means that the legal basis for the specific legislative measures that this study covers is subject to the national laws of each Member State and to the specific rules or user terms that the administrator of each ccTLD has laid down.

The mapping and analysis of the fourth topic on legislative measures aimed at the entities that host suspected IPR infringing content, also revealed a rather fragmented, overall picture. On the one hand, the exemption from liability of hosting providers that is covered by Article 14(1) of the Directive on electronic commerce has been implemented into the laws of all Member States. On the other hand, the possibility to require a hosting provider to suspend the existing account of a suspected infringer is not subject to specific EU legislation and the mapping shows that this legal measure is either not available or the availability is unresolved in almost half of the Member States. The situation is even more fragmented when it comes to the possibility to prevent suspected infringers from opening new accounts with the hosting service when a previous account has been suspended. This legal measure is either not available or its availability is unclear or subject to legal debate in over half of the Member States.

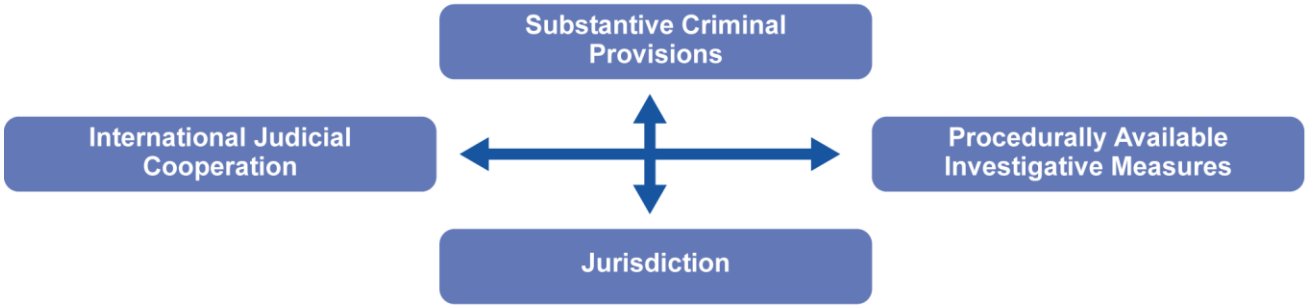
As regards the *criminal legislative measures*, the mapping and analysis also show both EU-wide commonalities and national differences.

Both the EIO and the EAW apply in principle certain types of IPR infringements, namely counterfeiting and piracy of products and as regards the EAW also computer related crimes. However, the basic requirement of the EIO and the EAW is that the offence is subject to a maximum period of at least three years of imprisonment in the issuing country, and since the maximum sentence in cases of counterfeiting and piracy is not three years in all Member States (see further below), this factor, among others, may limit the application of the EIO and the EAW by the competent authorities in the Member States in relation to IPR infringements.

The two most recently adopted anti-money laundering instruments, namely 'The Fourth Anti-Money Laundering Directive' and 'The Fund Transfers Regulation', cover proceeds originating from most types of criminal activities. The instruments do in principle cover proceeds originating from online IPR infringements, but at present there appears to be only one concrete example of this namely the SweFilmer case.

The topics explored in Chapter 8.9 of this study are aspects on the criminal sanctions in cases of IPR infringements that are laid down in the national laws of the Member States. Criminal sanctions are not subject to harmonisation at EU level, and the mapping shows that the type of penalties and the maximum penalties for IPR infringements vary considerably from Member State to Member State. Maximum custodial sentences, where those are applicable, vary from two to 10 years and also when it comes to such issues as whether negligent infringements are punishable and whether legal persons can be held liable for criminal infringements, the legal situation in the Member States is far from uniform.

FIGURE 41 — LEGISLATIVE FRAMEWORK FOR CRIMINAL ENFORCEMENT IN REGARDS TO IP CRIME



9. IDENTIFICATION OF FUTURE CHALLENGES

The internet and its technology stack is not standing still, rather it is under constant development. Mega trends such as machine learning and artificial intelligence, connected devices (IOT - Internet of Things), the blockchain technology, 3D printing and the like are likely to move some known internet related phenomena to other areas and give rise to new opportunities and challenges.

Technological advancements have impacted and are likely to continue to impact both the enforcement of IPRs online as well as the ways to infringe IPRs, for example via dissemination of unlawful copies of works or products. Whereas it is by the nature of a technology-neutral legislative framework neither desirable nor feasible to take into consideration all possible technological advancements, it is helpful to have a couple of developments on the radar. Given the evolving character of technologies and their adoption, the following list is not exhaustive but merely attempts to sketch some potential tendencies.

Continued growth of the internet user base

The global internet user base is growing flat at +10 % year on year over the last five years and currently has 46 % penetration at 3.4 billion users[172]. The smartphone installed base is at 2.8 billion users, with strong growth over the last decade and significantly slower growth more recently[173]. Thus, the internet user base is likely to continue to grow, with its biggest increase outside the EU and the western world. Online streaming platforms like Spotify, YouTube or Netflix have worked as catalysts for the internet-driven evolution of the music and video business and have arguably contributed to a decrease in the infringement of related IPRs. Novel business models, user patterns etc. are more likely to evolve outside the jurisdictional scope of the EU in the future. Additionally, more and more devices are connected to the internet, both based on growth in the user base and an increase in connected devices (internet of Things), which might give rise to novel challenges.

Evolving legal framework

The legal framework for the protection of IPRs is not static. Novel subjects or uses might lead to regulation and changing rights (e.g. in connection to the European Commission's proposals around copyright in the Digital Single Market or the novel nature of works generated by artificial intelligence). Any change in the substantive rights is also likely to incur changes on the enforcement side.

[172] http://www.kpcb.com/internet-trends

[173] http://www.kpcb.com/internet-trends

Non-judicial enforcement mechanisms

In the online landscape, an increasing tendency towards non-judicial takedown mechanisms put in place on a voluntary basis can be observed. Often times these voluntary mechanisms, for example in the form of 'trusted notifier' or 'trusted flagger' systems, are suggested by rights holders or their industry organisations and enshrined in agreements or Memorandum of Understandings with the respective intermediaries. In such a mechanism, a privileged notification channel is provided to parties, which are particularly knowledgeable or have particular expertise to identify unlawful content. Examples for such notifiers can range from individual or organised networks of private organisations, civil society organisations and semi-public bodies, to public authorities. In March 2018, the European Commission endorsed such voluntary mechanisms on all types of illegal content as well as on terrorist content in its Recommendation (EU) 2018/334 directed towards Member States and hosting service providers [174].

On the one side, these enforcement mechanisms could lead to the faster takedown of unlawful content and the relief of public enforcement bodies. On the other side, these mechanisms come with potential challenges on the impartiality of the notifiers, chilling effects or the rule of law. In the absence of legislation and the existing rules on intermediary liability, there exists also a certain degree of legal uncertainty.

Automated identification and/or enforcement

Recent and upcoming technological advancements, for example in algorithms related to pattern recognition and the analysis of big data, might refine existing modes and give rise to new modes of identifying infringing content on the internet (filter technologies). Similarly, novel technology could facilitate the automatic enforcement of IPRs. These developments are likely to stretch beyond the online environment (e.g. autonomous robots that search shipping containers etc.).

The use of such technology could, for example, lead to a faster and less resource heavy identification and/or enforcement. Despite the growing body of open source algorithms, such advanced technology is likely to continue to be resource heavy to develop. Additionally, the use of such technology might come with challenges as regards oversight and the rule of law, as well as the threat of chilling effects and over- or under-filtering and its compatibility with the existing legal framework [175].

[174] European Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online. See also the Commission's previous Communication COM(2017) 555 final of 28 September 2017 on Tackling Illegal Content Online, towards an enhanced responsibility of online platforms.

[175] In the online copyright environment, the European Commission recently suggested introducing measures by online platforms where large numbers of works are uploaded by their users to ensure the functioning of licensing agreements e.g. by using 'effective content recognition technologies', see Article 13, European Commission, Proposal for a Directive on copyright in the Digital Single Market, Brussels, 14 September 2016, COM(2016) 593 final.

Decentralisation

File sharing and streaming have moved from statically hosted to a decentralised system (e.g. via the BitTorrent protocol for peer-to-peer sharing). Further decentralisation of the internet both on the infrastructure and on the application layer can be desirable for a variety of reasons (robust infrastructure, censorship-resistant, etc.), but could also pose difficulties for the enforcement of IPR rights in distributed systems. Notably, current blockchain developments are likely to lead to an increased focus on the further development of decentralised systems.

Blockchain technology could, for example, be used in the context of works databases to store rights holder information in a distributed ledger. These databases could potentially come with efficiency gains both on remuneration for use of works and enforcement of rights.

Another example of blockchain technology could be the reduction of use of intermediaries for transactions, for example, blockchain-based DNS alternatives or decentralised marketplaces, which could make the enforcement of IPRs more challenging.

Development of parallel infrastructures and novel technologies

In light of technological advancements, also parallel infrastructures might emerge or grow, such as the so-called darknet[176]. A further example are blockchain-based alternative DNS-approaches, which could replace or supplement the existing DNS-system. The development of parallel infrastructures could provide additional challenges in the enforcement of IPRs.

[176] See the definition of 'darknet' on p. 14 in 'Research on Online Business Models Infringing Intellectual Property Rights. Phase 1'.

10. BIBLIOGRAPHY AND REFERENCES

EUIPO, Study on voluntary collaboration practices in addressing online infringements of trade mark rights, design rights, copyright and rights related to copyright, September 2016, accessible at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Research%20and%20sudies/study_voluntary_collaboration_practices_en.pdf (last accessed 23 February 2018).

EUIPO, 'Research on Online Business Models Infringing IPRs. Phase 1', July 2016, accessible at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf (last accessed 23 February 2018).

EUIPO, 'Research on Online Business Models Infringing Intellectual Property Rights. Phase 2', 2017, accessible at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Research_on_Online_Business_Models_Infringing_IP_Rights.pdf (last accessed 23 February 2018).

Europol and EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union', June 2017, accessible at: https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union (last accessed 23 February 2018).

INTA, 'Criminal Prosecution of Counterfeiting and Piracy in Member States of the European Union', February 2010, accessible at: http://www.inta.org/Advocacy/Documents/INTAEUCriminalSanctions20082009.pdf (last accessed 23 February 2018).

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Digital Single Market Strategy for Europe', COM(2015) 192 final.

Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, 'Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights', COM(2017) 708.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Tackling Illegal Content Online Towards an enhanced responsibility of online platforms', COM(2017) 555 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Online Platforms and the Digital Single Market. Opportunities and Challenges for Europe', COM(2016) 288.

Michel Vivant (ed.): 'European Case Law on infringements of intellectual property rights', Bruylant, 2016.

Knud Wallberg, 'Notice and takedown of counterfeit goods in the Digital Single Market: a balancing of fundamental rights', Journal of Intellectual Property Law & Practice, Volume 12, Issue 11, 1 November 2017, Pages 922-936.

Knud Wallberg, 'Recent Developments in Domain Name Law and Practice under the .dk Top Level Domain', NIR 1, 2017, p. 40 ff.

Lasse Lund Madsen, 'Edition som efterforskningsmiddel – med særlig henblik på internetrelaterede bedragerisager', U.2017B.205, p. 207.

Perel (Filmar), Maayan and Elkin-Koren, Niva, 'Accountability in Algorithmic Copyright Enforcement', February 21, 2016, Stanford Technology Law Review, Forthcoming. Available at: SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2607910.

World Intellectual Property Organization (WIPO), 'WIPO Cybersquatting Cases Hit Record in 2016, Driven by New Top-Level Domain Names', 16 March 2017, accessible at: http://www.wipo.int/pressroom/en/articles/2017/article_0003.html (last accessed 23 February 2018).

CJEU Cases

Case C-657/11, *Belgian Electronic Sorting Technology NV* v *Bert Peelaers & Visys NV*, EU:C:2013:516.

Case C-236/08, *Google France SARL*, EU:C:2010:159.

Case C-582/14, *Patrick Beyer* v *Bundesrepublik Deutschland*, EU:C:2016:779.

Case C-324/09, *Scarlet Extended SA* v *SABAM*, EU:C:2011:711.

Case C-324/09, *L'Oréal* v *eBay*, EU:C:2011:474.

Joined Cases C-585/08 and C-144/09, *Pammer and Hotel Alpenhof*, EU:C:2010:740.

11. LIST OF ABBREVIATIONS

ADR	Alternative dispute resolution
ccTLD	Country code top-level domains
CJEU	Court of Justice of the European Union
DNS	Domain name system
EAW	European Arrest Warrant
ECTA	European Communities Trade Mark Association
EIO	European Investigation Order
EUIPO	European Union Intellectual Property Office
EUTMR	European Trade Mark Regulation
ICANN	Internet Corporation for Assigned Names and Numbers
IP address	Internet protocol address
IPRED	Directive on Enforcement of Intellectual Property Rights
IPRs	Intellectual property rights
NSMs	Name server managers
NTD	Notice and takedown
SOCTA	Serious and Organised Crime Threat Assessment
TMDIR	Trade Marks Directive

12. LIST OF FIGURES

13. APPENDICES

CONTENT APPENDICES

13.1 Annex A: Questionnaire on civil legislative measures

UNIVERSITY OF COPENHAGEN
FACULTY OF LAW

EUIPO
Study on legislative measures related to online IPR infringements

Mapping of existing legislative measures available to combat and prevent online IPR infringements

National report for

[country]

Provided by: *[name]*
[title, position and workplace]

1

Table of contents

Purpose and Scope of the Study and of this Questionnaire

The overall purpose of the study is to identify and analyse those legislative measures adopted in the European Union member states that are applicable to enforcement of IP rights in a digital context. The study will be limited to measures which are suitable for collection of evidence and disruption of the infringement of trademark, copyright and related rights.

Furthermore, the study will be limited to collecting information on the following: to what extent can the relevant legislative measures be applied in situations that may involve one or more of the following eight, specific topics and related sub-topics:

The present questionnaire is limited to civil measures and therefore only covers topics 1 to 4.

TOPIC	SUB-TOPICS
1. Account Information	- Retrieval of information from hosting providers, internet service providers, social media networks and other intermediaries on: - The account holder contact information (the challenge of false contact information) - IP-address - WHOIS-information
2. Blocking of access to websites	- Website hosted in other EU-member states - Website hosted in non-EU member states
3. Domain name actions	- Types of actions (suspension, transfer, etc.) - Towards the Registry - Towards the Registrar - Towards the Registrant
4. Actions targeted at hosts	Actors hosting or advertising infringing material: - The workings of notice and takedowns of concrete listings - Suspension, blocking etc. of specific vendor accounts - Suspension, blocking etc. of future accounts of a specific account holder
5. Investigation order	- Obtaining evidence in other EU member states (Directive on European Evidence Order)
6. Extradition	Extradition of own nationals - Extradition of foreigners
7. Money laundering	
8. Criminal sanctions	- Maximum sentences - Confiscation - Prohibition of future business. Period of time.

The questionnaire is based on the premise that all member states have implemented the Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (hereby, 'IP Enforcement Directive). It also assumes that these provisions apply to online infringements of trademarks, copyrights and related rights.

Definitions and delimitations

- The questionnaire has been divided in parts that reflect these immediately identified topics;
- Focus on measures that are suitable for collection of evidence and disruption of infringements;
- It is limited to infringements that takes place online; and
- Only covers infringements of trademarks, copyrights and related rights.

Guidelines for answering the questionnaire

Quoting and citing legislation and jurisprudence:

- Mention legal instruments by official title, followed if possible by English translation (reference the author/entity responsible for the translation).

National or /EU/International Law:

- The legislative origin of a measure may be difficult to determine precisely. In such case consider the measure as national and quote the provision.

Additional comments:

- Here you may provide additional information you find relevant to this study, for example: legal provisions, judicial decisions, legal interpretation controversies, and statistics or data collections.

For any questions contact the Study Coordinator:
Ana Nordberg, PhD
Email: ana.nordberg@jur.ku.dk
Tel. 0045 35 32 35 86

Section A. EU Harmonized legal measures applicable to online infringement of Intellectual Property rights

Question 1: Measures applicable for obtaining account information

Can an online intermediary be asked to disclose account information on a particular customer? *(For the purpose of this question, intermediaries include among others: internet service providers, internet hosting provides, social media networks, online platforms and market places and other intermediaries)*
Yes No Unresolved Yes but only under certain circumstances (please explain):
If yes or only in certain circumstances**, can these measures be applied to obtain the following information from the concerned intermediary:**
The contact information on the holder a specific account on the online network/platform (f.ex. a social media network/platform or a digital marketplace)? Yes No Unresolved Yes but only under certain circumstances (please explain): The contact information on the person or entity that uses an IP-address provided by the intermediary (f.ex. an internet service provider)? Yes No Unresolved Yes but only under certain circumstances (please explain): The contact information on the person or entity that makes a server available under an IP-address provided by the intermediary (f.ex. an internet hosting provider)? Yes No Unresolved

5

Yes but only under certain circumstances (please explain):

The 'real' contact information of the registrant of a domain name if the registrant is anonymous or uses a privacy service or the like in the publicly available WHOIS?

Yes No Unresolved

Yes but only under certain circumstances (please explain):

What are the legislative bases for these actions?

1 National provision that implements art. 7 of the IP Enforcement Directive regarding preserving of evidence

2 National provision that implements art. 8 of the IP Enforcement Directive regarding the right to information

3 Specific national legislation that does not implement provisions of the IP Enforcement Directive

Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English.

Additional remarks or comments (if any):

6

Question 2: Measures applicable for blocking access to websites

Can an order blocking access to websites be issued?
Yes No Unresolved Yes but only under certain circumstances (please explain):
If yes or only in certain circumstances**, can these measures be applied to block access to websites in the following situations:**
Websites hosted in the EU-member state itself? Yes No Unresolved Yes but only under certain circumstances (please explain): Websites hosted in another EU-member state? Yes No Unresolved Yes but only under certain circumstances (please explain): Websites hosted in a non-EU-member state? Yes No Unresolved Yes but only under certain circumstances (please explain):
What are the legislative bases for these actions?

7

1 National provision that implements art. 9 of the IP Enforcement Directive regarding provisional and precautionary measures

2 National provision that implements art. 10 of the IP Enforcement Directive regarding corrective measures

3 National provision that implements art. 11 of the IP Enforcement Directive regarding (permanent) injunctions

4 Specific national legislation that does not implement provisions of the IP Enforcement Directive

Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English:

Additional remarks or comments (if any):

8

Question 3: Measures applicable in domain name actions

Can the Registry of your country code top level domain be ordered to implement one or more of the following actions:
Transfer of a disputed domain name (to the IPR owner)? Yes No Unresolved Yes but only under certain circumstances (please explain): Suspension of a disputed domain name (meaning that the domain name servers related to the disputed domain name are inactivated)? Yes No Unresolved Yes but only under certain circumstances (please explain): Deletion of a disputed domain name? Yes No Unresolved Yes but only under certain circumstances (please explain): Other measures, if any *(please explain):*
What are the legislative bases for these actions?
1 National provision that implements art. 9 of the IP Enforcement Directive regarding provisional and precautionary measures 2 National provision that implements art. 11 of the IP Enforcement Directive regarding (permanent) injunctions

9

3 Specific national legislation that does not implement provisions of the IP Enforcement Directive

Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English:

Additional remarks or comments (if any):

Can a national authority order the Registrar of a domain name to:
(Your answer should presume that the national court has jurisdiction. Thus, it is not relevant whether the disputed domain name is registered under your local ccTLD or not).

Transfer a disputed domain name (to the IPR owner)?

Yes No Unresolved

Yes but only under certain circumstances (please explain):

Delete a disputed domain name?

Yes No Unresolved

Yes but only under certain circumstances (please explain):

Other measures, if any *(please explain):*

10

What are the legislative bases for these actions?
1 National provision that implements art. 9 of the IP Enforcement Directive regarding provisional and precautionary measures 2 National provision that implements art. 11 of the IP Enforcement Directive regarding (permanent) injunctions 3 Specific national legislation that does not implement provisions of the IP Enforcement Directive *Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English*:
Additional remarks or comments (if any):

Can a national authority order the Registrant of a domain name to: *(Your answer should presume that the national court has jurisdiction. Thus, it is not relevant whether the disputed domain name is registered under your local ccTLD or not).*
Transfer a disputed domain name (to the IPR owner)? Yes No Unresolved Yes but only under certain circumstances (please explain): Delete a disputed domain name? Yes No Unresolved Yes but only under certain circumstances (please explain):

11

Other measures, if any *(please explain):*
What are the legislative bases for these actions?
1 National provision that implements art. 9 of the IP Enforcement Directive regarding provisional and precautionary measures 2 National provision that implements art. 11 of the IP Enforcement Directive regarding (permanent) injunctions 3 Specific national legislation that does not implement provisions of the IP Enforcement Directive *Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English*:
Additional remarks or comments (if any):

12

Question 4: Measures applicable for actions targeted at hosts

Can an online intermediary whose platform is being used to host or to advertise IPR infringing goods, be ordered to "take down" an infringing sales offer or an infringing advertisement?
Yes No Unresolved Yes but only under certain circumstances (please explain):
What are the legislative bases for these actions?
1 National provision that implements art. 9 of the IP Enforcement Directive regarding provisional and precautionary measures 2 National provision that implements art. 11, 3rd sentence of the IP Enforcement Directive regarding (permanent) injunctions 4 Specific national legislation that does not implement provisions of the IP Enforcement Directive *Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English*:
Additional remarks or comments (if any):

Can an online intermediary, whose platform is being used to host or to advertise IPR infringing goods, be ordered to suspend or block the account of the infringing vendor or advertiser?
Yes No Unresolved Yes but only under certain circumstances (please explain):

13

What are the legislative bases for these actions?
1 National provision that implements art. 9 of the IP Enforcement Directive regarding provisional and precautionary measures 2 National provision that implements art. 11, 3rd sentence of the IP Enforcement Directive regarding (permanent) injunctions 4 Specific national legislation that does not implement provisions of the IP Enforcement Directive *Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English*:
Additional remarks or comments (if any):

Can an online intermediary, whose platform is being used to host or to advertise IPR infringing goods, be ordered to block or otherwise prevent the opening of future accounts by a specific vendor or advertiser?
Yes No Unresolved Yes but only under certain circumstances (please explain):
What are the legislative bases for these actions?

14

1 National provision that implements art. 9 of the IP Enforcement Directive regarding provisional and precautionary measures 2 National provision that implements art. 10 of the IP Enforcement Directive regarding corrective measures 3 National provision that implements art. 11, 3rd sentence of the IP Enforcement Directive regarding (permanent) injunctions 4 Specific national legislation that does not implement provisions of the IP Enforcement Directive *Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English*:
Additional remarks or comments (if any):

15

Section B. Specific national legislative measures

This section refers to legislation which does not implement EU legislation, such as for example the provisions of the IP Enforcement Directive or any other EU legislation. We are particularly interested in national legal innovation and developments in the field of online enforcement of IPR's.

Please describe any eventual national civil enforcement actions and mechanisms not previously mentioned that can be used to disrupt the online infringement of IPR's.

Copy/paste and fill in the table as many times as appropriate.

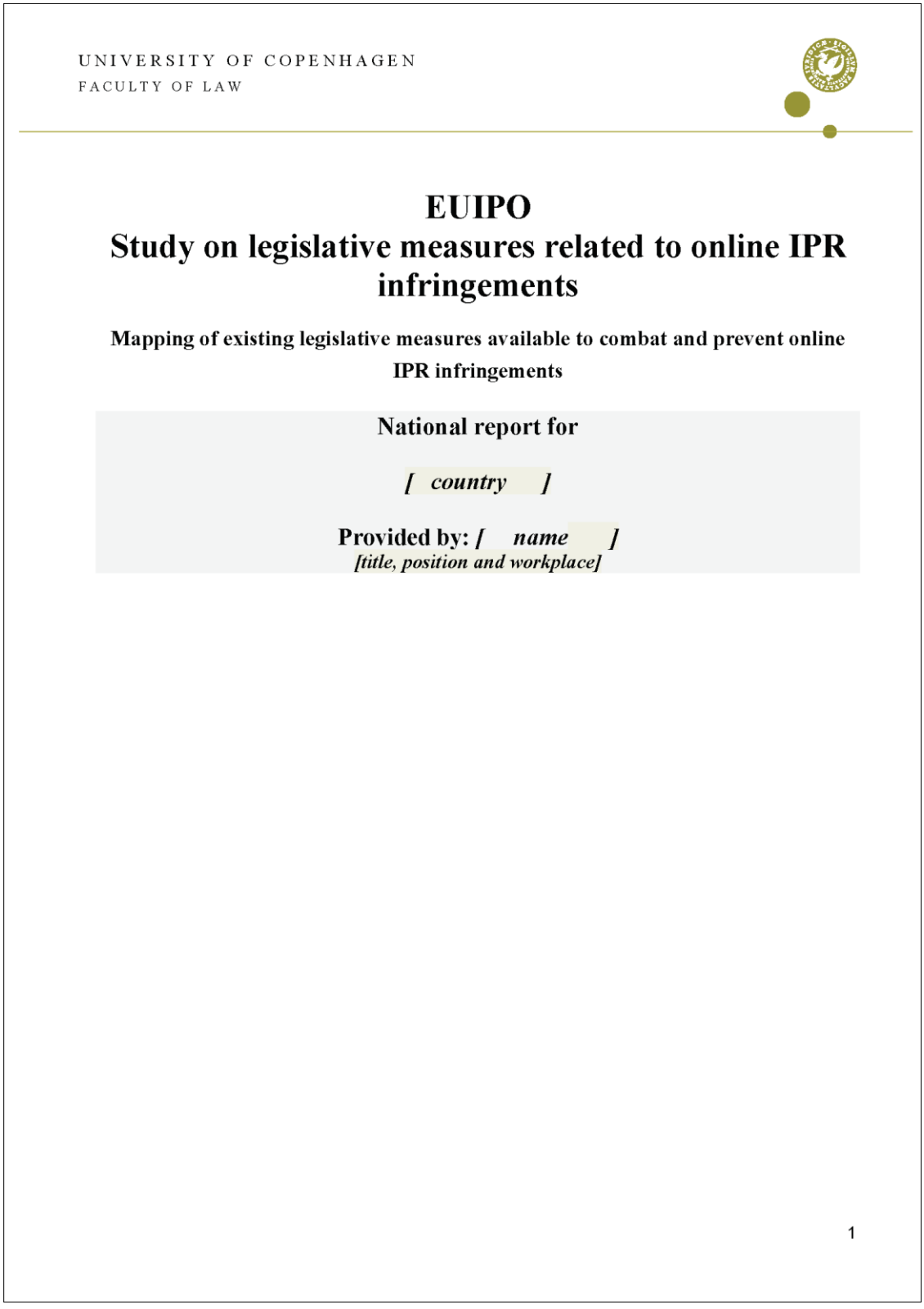
Title/official designation:
Purpose, content and relevance to enforcement of IPR against online infringements. *Briefly describe and quote the legal provisions, include article, legal instrument and the field of law (in English).*

Title/official designation:
Purpose, content and relevance to enforcement of IPR against online infringements. *Briefly describe and quote the legal provisions, include article, legal instrument and the field of law (in English).*

Title/official designation:
Purpose, content and relevance to enforcement of IPR against online infringements. *Briefly describe and quote the legal provisions, include article, legal instrument and the field of law (in English).*

16

13.2 Annex B: Questionnaire on criminal legislative measures



UNIVERSITY OF COPENHAGEN
FACULTY OF LAW

EUIPO
Study on legislative measures related to online IPR infringements

Mapping of existing legislative measures available to combat and prevent online IPR infringements

National report for

[country]

Provided by: *[name]*
[title, position and workplace]

1

Table of contents

Purpose and Scope of the Study and of the Questionnaire

The main purpose of the study is to identify and analyse the legislative measures adopted in the European Union member states applicable to IP rights enforcement in a digital context. Namely, measures suitable for collection of evidence and disruption of infringements. The study will be limited to the infringement of trademark, copyright and related rights.

The questionnaire is based on the premise that all member states have implemented the relevant EU legislation. It also assumes that these provisions apply to online infringements of trademarks, copyrights and related rights.

The present study is limited to collecting information on the following: to what extent can the relevant legislative measures be applied in situations that may involve one or more of the following eight, specific topics and related sub-topics:

The present questionnaire is limited to Criminal and Administrative legal measures relating to these topics:

TOPIC	SUB-TOPICS
1. Account Information	- Retrieval of information from social media platforms and other intermediaries on: - The account holder contact information (the challenge of false contact information) - IP-address - WHOIS-information
2. Blocking of access to websites	- Website hosted in other EU-member states - Website hosted in non-EU member states
3. Domain name actions	- Types of actions (suspension, transfer, etc.) - Towards the Registry - Towards the Registrar - Towards the Registrant
4. Actions targeted at hosts	Actors hosting or advertising infringing material: - The workings of notice and takedowns of concrete listings - Suspension, blocking etc. of specific vendor accounts - Suspension, blocking etc. of future accounts of a specific account holder
5. International legal cooperation	- Obtaining evidence in other EU member states (Directive on European Evidence Order)
6. Extradition	Extradition of own nationals - Extradition of foreigners
7. Money laundering	
8. Criminal sanctions	- Maximum sentences - Confiscation - Prohibition of future business. Period of time.

Definitions and delimitations

- The questionnaire has been divided in parts that reflect these immediately identified topics;
- Focus on measures that are suitable for collection of evidence and disruption of infringements;

3

- It is limited to infringements that takes place online; and
- Only covers infringements of trademarks, copyrights and related rights.

Guidelines for answering the questionnaire

Quoting and citing legislation and jurisprudence:

- Mention legal instruments by official title, followed if possible by English translation (reference the author/entity responsible for the translation).

National or /EU/International Law:

- The legislative origin of a measure may be difficult to determine precisely. In such case consider the measure as national and quote the provision.

Additional comments:

- Here you may provide additional information you find relevant to this study, for example: legal provisions, judicial decisions, legal interpretation controversies, and statistics or data collections.

For any questions contact the Study Coordinator:
Ana Nordberg, PhD
Email: ana.nordberg@jur.ku.dk
Tel. 0045 35 32 35 86

Section A. Administrative and criminal measures applicable to online infringement of Intellectual Property rights

Question 1: Measures applicable for obtaining account information:

Can an online intermediary be asked to disclose account information on a particular customer? *(For the purpose of this question, intermediaries include among others: internet service providers, internet hosting provides, social media networks, online platforms and market places and other intermediaries)*
Yes No Unresolved Yes but only under certain circumstances (please explain):
If yes or only in certain circumstances**, can these measures be applied to obtain the following information from the concerned intermediary:**
The contact information on the holder a specific account on the online network/platform (f.ex. a social media network/platform or a digital marketplace)? Yes No Unresolved Yes but only under certain circumstances (please explain): The contact information on the person or entity that uses an IP-address provided by the intermediary (f.ex. an internet service provider)? Yes No Unresolved Yes but only under certain circumstances (please explain): The contact information on the person or entity that makes a server available under an IP-address provided by the intermediary (f.ex. an internet hosting provider)?

5

Yes No Unresolved Yes but only under certain circumstances (please explain): The 'real' contact information of the registrant of a domain name if the registrant is anonymous or uses a privacy service or the like in the publicly available WHOIS? Yes No Unresolved Yes but only under certain circumstances (please explain):
What are the legislative bases for these actions?
Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English.
Additional remarks or comments (if any):

6

Question 2: Measures applicable for blocking access to websites:

Can an order blocking access to websites be issued?
Yes No Unresolved Yes, but only under certain circumstances (please explain):
If yes, can these measures be applied to block access to websites in the following situations:
Websites hosted in the EU-member state territory? Yes No Unresolved (please explain): Websites hosted in another EU-member state? Yes No Unresolved (please explain): Websites hosted in a non-EU-member state? Yes No Unresolved (please explain):
What are the legislative bases for these actions?
Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English:

7

Additional remarks or comments (if any):

8

Question 3: Measures applicable in domain name actions:

Can the Registry of your country code top level domain be ordered to implement one or more of the following actions:
Transfer of a disputed domain name (to the IPR owner)? Yes No Unresolved Yes but only under certain circumstances (please explain): Suspension of a disputed domain name (meaning that the domain name servers related to the disputed domain name are inactivated)? Yes No Unresolved Yes but only under certain circumstances (please explain): Deletion of a disputed domain name? Yes No Unresolved Yes but only under certain circumstances (please explain): Other measures, if any *(please explain):*
What are the legislative bases for these actions?
Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English:

9

Additional remarks or comments (if any):

Can a national authority order the <u>Registrar</u> of a domain name to: *(Your answer should presume that the national court has jurisdiction. Thus, it is not relevant whether the disputed domain name is registered under your local ccTLD or not).*
Transfer a disputed domain name (to the IPR owner)? Yes No Unresolved Yes but only under certain circumstances (please explain): Delete a disputed domain name? Yes No Unresolved Yes but only under certain circumstances (please explain): Other measures, if any *(please explain):*
What are the legislative bases for these actions?
Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English:
Additional remarks or comments (if any):

10

Can a national authority order the Registrant of a domain name to: *(Your answer should presume that the national court has jurisdiction. Thus, it is not relevant whether the disputed domain name is registered under your local ccTLD or not).*
Transfer a disputed domain name (to the IPR owner)? Yes No Unresolved Yes but only under certain circumstances (please explain): Delete a disputed domain name? Yes No Unresolved Yes but only under certain circumstances (please explain): Other measures, if any *(please explain):*
What are the legislative bases for these actions?
Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English:
Additional remarks or comments (if any):

11

Question 4: Measures applicable for actions targeted at hosts

Can an online intermediary whose platform is being used to host or to advertise IPR infringing goods, be ordered to "take down" an infringing sales offer or an infringing advertisement?
Yes No Unresolved Yes but only under certain circumstances (please explain):
What are the legislative bases for these actions?
Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English:
Additional remarks or comments (if any):

Can an online intermediary, whose platform is being used to host or to advertise IPR infringing goods, be ordered to suspend or block the account of the infringing vendor or advertiser?
Yes No Unresolved Yes but only under certain circumstances (please explain):
What are the legislative bases for these actions?

13

Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English:
Additional remarks or comments (if any):

Can an online intermediary, whose platform is being used to host or to advertise IPR infringing goods, be ordered to block or otherwise prevent the opening of <u>future accounts</u> by a specific vendor or advertiser?
Yes No Unresolved Yes but only under certain circumstances (please explain):
What are the legislative bases for these actions?
Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English:
Additional remarks or comments (if any):

14

Section B. EU Judicial cooperation

Question 5: European Investigation Order

Can a European Investigation Order be issued or requested by the authorities in your country in relation to online infringements of intellectual property rights?
Yes No Unresolved or only in certain circumstances (please explain):
If yes or under certain circumstances, is double criminality required? Yes No Unresolved or only in certain circumstances (please explain):
If yes or under certain circumstances, can these measures be used to:
Request information concerning bank account holders/financial transactions? Yes No Unresolved or only under certain circumstances (please explain): Freeze or confiscate bank accounts: Yes No Unresolved or only under certain circumstances (please explain): Locate and seize servers and other equipment used in infringing activities? Yes No Unresolved or only under certain circumstances (please explain):

15

Intercept and seize Counterfeited products before they reach the consumer?

Yes No

Unresolved or only under certain circumstances (please explain):

Additional remarks or comments (if any):

16

Question 6: European Arrest warrant

Can a European Arrest Warrant be issued or requested by the authorities in your country in relation to online infringements of intellectual property rights?
Yes No Unresolved or only in certain circumstances (please explain):
If yes or under certain circumstances, is double criminality required? Yes No Unresolved or only in certain circumstances (please explain):
If yes or under certain circumstances, can a European Arrest Warrant be issued to extradite national citizens of the executing member state?
Yes No Unresolved or only under certain circumstances (please explain):
If yes, can a European Arrest Warrant be issued to extradite foreign citizens with permanent residence in the executing member state?
Yes No Unresolved or only under certain circumstances (please explain):

17

Question 7: Money Laundering

Has the Money laundering Directive been transposed to national law and can it apply to online infringements of intellectual property rights?
Yes **No** Unresolved or only in certain circumstances (please explain):
Additional remarks or comments (if any):

18

Section C. National criminal and administrative enforcement

Question 8: Administrative measures

Does your jurisdiction contemplates additional administrative procedures to stop or disrupt online infringement of Intellectual Property rights?
Yes **No** *If yes, briefly describe the measures and quote legal provisions (you may refer back to previous answers if already mentioned in Section A):* Unresolved or only in certain circumstances (please explain):
What are the legislative bases for these actions?
Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English:
Additional remarks or comments (if any):

Question 9: Criminal and Administrative sanctions:

Does national law contemplate accessory or alternative penalties such as seizure of goods and property (including domain names); interdiction of future business/professional activity, or publicity of sentences?
Yes **No** *If yes, briefly describe the measures and quote legal provisions (you may refer back to previous answers if already mentioned A)):* Unresolved or only in certain circumstances (please explain):

19

What are the legislative bases for these actions?
Briefly describe and quote the legal provisions. Please include a copy of the legal instrument, preferably in English:
What are the maximum penalties per type of online IPR infringement? *Please indicate per each crime type, if it is a public, semi-public or private crime.*
Trademark infringement
Copyright infringement
What are the time limits for penal enforcement of online IPRs infringement? *Please indicate all eventual relevant time limits precluding further legal action (for example: limits to formalise a complaint, initiate proceedings, deduct accusation, issue a conviction, etc.)*
Trademark infringement
Copyright infringement
Does national penal law punish negligent online IPR infringement?
Yes **No** *If yes, quote the legal provision(s) in English:* Unresolved or only in certain circumstances (please explain):
Does national penal law punish also online IPR infringements at a non-commercial scale?

20

Yes **No** *If yes, quote the legal provision(s) in English:* Unresolved or only in certain circumstances (please explain):
Does national penal law allow objective criminal liability for online IPR Infringement?
Yes **No** *If yes, quote the legal provision(s) in English:* Unresolved or only in certain circumstances (please explain):
Can legal persons be held criminally liable for online IPR infringements (including intermediaries)? *Briefly describe and quote legal provisions, include article, legal instrument and field of law (in English).*
Yes **No** *If yes, quote the legal provision(s) in English:* Unresolved or only in certain circumstances (please explain):
Additional remarks or comments (if any):

21

Section D. Specific national criminal or administrative enforcement actions

This section refers to legislation that does not implement EU provisions. We are particularly interested in national legal innovation in the field of online enforcement of IPR's.

Please describe any eventual national criminal or administrative enforcement actions and mechanisms not previously mentioned that can be used to disrupt the online infringement of IPR's.

Copy/paste and fill in the table as many times as appropriate.

Title/official designation:
Purpose, content and relevance to enforcement of IPR against online infringements. *Briefly describe and quote the legal provisions, include article, legal instrument and the field of law (in English).*
Who can request and what authority can order these measures? **(***Please indicate separately for different types of IPRs infringement considered criminal offenses under your jurisdiction, if these measures can be requested by the right holder, public prosecutor, police and/or other enforcement authority, and what authority can/should issue the corresponding order)*
Comments (if any):

22

ISBN 978-92-9156-255-8 doi:10.2814/36519 TB-02-18-500-EN-N

STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE IPR INFRINGEMENTS