



Faculty of Law, University of Amsterdam
Institute for Information Law

P.O. Box 15514
1001 NA Amsterdam
The Netherlands
www.ivir.nl

Global Online Piracy Study Legal Background Report

João Pedro Quintais

Date July 2018

The research project was financed by Google. It has been conducted in full compliance with the Declaration of Scientific Independence as formulated by the Royal Dutch Academy of Science.

This Legal Background Report is part of the Global Online Piracy Study. The Study, its Annexes, and this Report are available for download at: <https://www.ivir.nl/>

Global Online Piracy Study **Legal Background Report**

Date July 2018

Author: João Pedro Quintais, Postdoctoral Researcher, Insitute for Information Law (IViR), Faculty of Law, University of Amsterdam

This Legal Background Report is based on 13 national questionnaires, reproduced in Annex 2, and prepared by the following authors: Brad Spitz (France); Franz Hofmann (Germany); Stef van Gompel (Netherlands); Tomasz Targosz (Poland); Raquel Xalabarder (Spain); Kacper Szkalej (Sweden); Christina Angelopoulos (UK); Allan Rocha Souza and Luca Schirru (Brazil); David Fewer (Canada); Alice Lee (Hong Kong); Henry Soelistyo (Indonesia); Tatsuhiro Ueno (Japan); Ning (Nontaya) Chulajata and Fabrice Mattei (Thailand). The authors' titles and affiliations, as well as the dates on which their reports were last updated are identified in Annex 2.

Research assistance for this report was provided by Nathalie Rodriguez and Jasmin Hohmann.

This Legal Background Report is part of the Global Online Piracy Study. The Study, its Annexes, and this Report are available for download at: <https://www.ivir.nl/>

CONTENTS

Abbreviations.....	5
Summary of findings.....	6
1. Introduction and Methodology.....	24
2. Legal Background: International and EU Copyright Law	25
2.1. International Law	25
Berne Convention.....	25
The TRIPS Agreement	26
The WIPO Treaties.....	27
2.2. EU law	28
InfoSoc Directive	30
Enforcement Directive	33
E-Commerce Directive (ECD)	34
3. Substantive rules on copyright infringement.....	36
3.1. Online acts qualified as copyright infringement.....	36
Downloading.....	36
Streaming	39
Stream-ripping.....	40
Uploading.....	41
Hyperlinking	42
Sale of Kodi boxes or similar devices	43
Other types of unauthorized use.....	45
Legal uncertainty areas.....	45
Summary Table	45
3.2. The relevance of different elements for infringement.....	45
3.3. Liability of online intermediaries.....	46
The notion of “intermediary” and safe-harbors in national law	46
Legal uncertainty on intermediary or secondary liability.....	54
3.4. Treatment of copyright infringement by minors.....	57
4. Enforcement measures, procedures, remedies, and sanctions.....	58
4.1. Enforcement measures available against users	59
Civil.....	59
Administrative.....	64
Criminal.....	67
Variation per type of content.....	70
4.2. Enforcement measures available against intermediaries.....	71
Civil.....	71
Administrative.....	75

Criminal.....	77
Variation per type of content.....	78
4.3. Differences in public and private enforcement per type of protected content	78
4.4. Disclosure of personal data in the context of enforcement	79
4.5. Entitlement to apply for enforcement measures.....	83
4.6. Most used and effective enforcement measures.....	85
ANNEX 1: LEGAL QUESTIONNAIRE	91
ANNEX 2: NATIONAL QUESTIONNAIRES – Responses to section 1 (online copyright infringement and enforcement in national law)	99
Questionnaire France	100
Questionnaire Germany	112
Questionnaire the Netherlands	127
Questionnaire Poland.....	138
Questionnaire Spain	151
Questionnaire Sweden	171
Questionnaire United Kingdom	199
Questionnaire Brazil	216
Questionnaire Canada	234
Questionnaire Hong Kong	250
Questionnaire Indonesia.....	260
Questionnaire Japan	273
Questionnaire Thailand.....	282
ANNEX 3: Summary Tables Question 3 – online acts qualified as copyright infringement	293
LEGISLATION AND CASES	307
International.....	307
European Union.....	307
Table of Cases Court of Justice Of The European Union (CJEU)	308

Abbreviations

AG	Advocate General
BC or Berne	Berne Convention for the Protection of Artistic and Literary Works
CMO(s)	Collective Rights Management Organization(s)
CJEU	Court of Justice of the European Union (former European Court of Justice (ECJ))
EU	European Union
EU Charter	Charter of Fundamental Rights of the European Union
IViR	Institute for Information Law at the University of Amsterdam
ISP	Internet Service Provider(s)
NPO	<i>Norwich Pharmacal</i> order
NTD	Notice-and-takedown
P2P	Peer-to-peer
RMI	Rights management information
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TPM(s)	Technological Protection Measure(s)
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Law
UK	United Kingdom
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organization
WIPO Treaties	The WCT and WPPT
WPPT	WIPO Performances and Phonograms Treaty
WTO	World Trade Organization

Note: Abbreviations to regional and national legislative instruments and court decisions can be found in the respective national questionnaires. Abbreviations of cases from the CJEU are found at the “Table of Cases...” section at the end of this report.

Summary of findings

This legal report is based on desk research and the analysis of questionnaires completed by legal experts in thirteen countries, including seven European Union (EU) member states (France, Germany, Netherlands, Poland, Spain, Sweden and United Kingdom), two American countries (Brazil and Canada), and four Asian countries (Hong Kong, Indonesia, Japan, and Thailand). The questionnaire concerns the legal status of online copyright infringement and enforcement under “national law”, a term that includes statute and case law. The questions concern two interrelated aspects: (1) substantive legal rules and (2) enforcement measures, procedures, remedies and sanctions.

LEGAL BACKGROUND

Copyright law is substantially harmonized by international law, which sets out basic rules and minimum standards on substantive copyright law and enforcement. The most relevant international treaties and conventions in copyright law are the Berne Convention for the Protection of Literary and Artistic Works (**BC**), the 1994 Agreement on Trade-Related Aspects of Intellectual Property Law (**TRIPS**) and, in relation to use over digital networks, the 1996 WIPO Copyright Treaty (**WCT**), and the WIPO Performances and Phonograms Treaty (**WPPT**).

All EU member states are parties to all international agreements. The EU as an organization is a member of TRIPS and the WIPO Treaties, making them binding on its institutions and Member States. All countries in the study are party to the BC and to the latest amended version of TRIPS. Most countries are party to the WIPO Treaties, with the exception of Brazil and Thailand, which are not members of either.

The BC sets out minimum standards regarding inter alia the protection of works and the rights of authors. The TRIPS sets out minimum standards concerning the availability, scope and use of intellectual property rights, including copyright and related rights. The minimum standards include protected subject matter, rights conferred, and permissible exceptions or limitations to those rights. Regarding copyright, TRIPS incorporates by reference most substantive provisions of the latest version of the BC, making them obligations under TRIPS as between its members. Furthermore, the Agreement includes obligations regarding subject matter and rights not covered by the BC. Finally, differently from the BC, TRIPS includes rules on enforcement procedures and subjects disputes between members concerning these obligations to WTO dispute settlement procedures.

The WCT and WPPT adapt copyright and related rights to the digital age. The WCT is a special agreement under the BC, incorporating by reference most of its substantive provisions and adding protected subject matter and substantive rights to the international minimum standards. Among the features of this treaty is the recognition of a broad reproduction right with application to the digital environment and a general right of communication to the public, including a making available prong covering interactive and on-demand use of digital content. The WPPT likewise extends to the digital age the standards of protection of the 1961 Rome Convention, including the recognition of a making available right for performers and phonogram producers. Both WIPO Treaties recognize in addition legal protection against the circumvention of technological protection measures (**TPMs**) and rights management information (**RMI**), as well as “light” provisions on enforcement of rights mandating contracting parties to adopt measures to ensure application of the treaties, although no specific measures are prescribed.

EU law

EU law has been subject to a high level of harmonization stemming from a large number of directives on copyright and related rights, the interpretation of which is determined by case law of the Court of Justice of the EU (**CJEU**). This copyright *acquis communautaire* often surpasses international

minimum standards of protection. For our purposes, the most relevant instruments are the InfoSoc Directive (2001), the Enforcement Directive (2004), and the E-Commerce Directive or “ECD” (2000). (The latter is not strictly part of the copyright *acquis*.)

The InfoSoc Directive implements the WIPO Treaties into EU law and adapts it to the information society. It recognizes exclusive rights applicable to online use, namely reproduction and communication to the public (including making available), as well as number of exceptions or limitations to the same. The case law of the CJEU traditionally interprets the exclusive rights broadly and the exceptions strictly. Particularly important is its case law on the right of communication to the public, which includes the consideration of elements of knowledge and commerciality in the assessment of primary liability.

The directive further provides WCT/WPPT-“plus” legal protection to TPM and RMI against circumvention and preparatory acts. Finally, the directive includes a provision on sanctions and remedies (implementing the WIPO Treaties), including a provision obligating member states to ensure that right holders can apply for injunctions against intermediaries whose services are used by a third party to infringe copyright, even if the intermediary is not itself directly liable for infringement. This provision has played a significant role in determining the liability of Internet Service Providers (ISPs), in articulation with the liability exemptions for intermediaries in the ECD. In essence, although national laws can determine the scope and procedures of injunctive relief, these are limited inter alia by the operation of fundamental rights recognized in the Charter of Fundamental Rights of the EU, leading to a fair balancing exercise.

The Enforcement Directive implements TRIPS and applies to all types of intellectual property rights. It deals exclusively with *civil* enforcement measures, procedures and remedies, including rules on standing, injunctions (interlocutory and final), damages, and codes of conduct for infringement.

In EU law, there’s no comprehensive harmonization of intermediary liability. The ECD contains conditional liability exemptions or “safe harbors” for certain types of intermediary services regarding claims for damages: mere conduit (or access), caching, and hosting. The directive further contains a prohibition on the imposition of “general” monitoring obligations on intermediaries. This regime does not prevent that intermediaries are required to take measures against the infringement of copyright, which may result from the possibility of injunctions against intermediaries under the InfoSoc Directive, as well as from the imposition of duties of care. In interpreting this constellation of provisions, the CJEU has noted that safe harbors require a sufficient degree of “neutrality” from the intermediary. This approach creates a grey area for the qualification of certain web 2.0 platforms as “neutral” / “passive” or “active” intermediaries for the purposes of the hosting safe harbor. Furthermore, it remains unclear what type of “specific” (as opposed to “general”) monitoring duties may be lawfully imposed on providers to prevent infringement. CJEU case law has not sufficiently clarified these uncertainties.

RULES ON COPYRIGHT INFRINGEMENT

Primary liability: Online acts infringing copyright

To determine the legal status of online use under national law we use a catalogue of online acts susceptible of infringing the exclusive rights of copyright holders. All the acts refer to the use of copyright-protected content from illegal/unauthorized sources or the provision of access to works made available without the permission of copyright holders. They are as follows: downloading; (passive) streaming; stream-ripping; uploading; hyperlinking; sale of kodi boxes or similar devices with pre-installed add-ons providing links to illegal/unauthorized sources. This list is supplemented by a catch-all category meant to include other activities that may infringe copyright specific to a national law.

Downloading: In most national laws, downloading from an illegal/unauthorized sources is unequivocally an act of direct copyright infringement of the exclusive right of reproduction, not privileged by a private use/copying limitation.

In the EU, although the legal status of the act has been clarified in the EU by the Court in *ACI Adam*, at least in Poland there is some uncertainty among scholars due to the failure to amend national law. In Brazil, the act is probably infringing but there is some uncertainty due to the lack of case law and the fact that criminal liability is expressly excluded for these acts. In Canada, the act is infringing except regarding musical sound recordings, as these are subject to a compensated private copying exception which does not expressly mention the legal status of the source of reproduction. In Hong Kong, the fair dealing defense may apply on a case-by-case basis to downloading depending on the purpose thereof (research, private study, criticism, review, news reporting or education) and whether certain requirements are met (acknowledgment and content removal). In Indonesia, non-commercial downloading will in many instances be covered by a general exception or “fair dealings” clause to the reproduction right. In Japan, this activity is only infringing regarding digital sound or video recordings and appears to require knowledge of the unlawful/unauthorized nature of the source.

(Passive) Streaming: By streaming we mean the reception or accessing of a stream by a user. Streaming of this type involves making a temporary and often transient copy of a work; if qualified as a reproduction, it may also be subject to an exception for these types of copies.

In the EU, most member states qualify this act as a reproduction. However, the Dutch and French experts make a more nuanced analysis, influenced by the specific facts of the CJEU case *Filmspeler*. Both experts argue that *Filmspeler* only applies if the stream is accessed through a kodi box or similar device with pre-installed add-ons that link to content made available online without the permission of rights holders; in other scenarios, streaming may not qualify as a reproduction. Where streaming is considered a reproduction, all European national laws follow *Filmspeler* and exclude the application of the temporary and transient copying exception to this activity, on the grounds that it does not meet the “lawful use” requirement.

The situation is different outside the EU. As a general remark, there is uncertainty across the board due to the absence of case law on this topic. With that in mind, both the Brazilian and Canadian experts argue for the likelihood that passive streaming is outside the scope of copyright due to its experiential nature. In Canada, even if the act is qualified as a reproduction, it would be likely privileged by an exception. The assessment is similar in Hong Kong and Japan. Only in Indonesia and Thailand is this activity probably infringing, but this conclusion is uncertain, due to the lack of specific case law on the matter.

Stream-ripping: For the most part, stream-ripping from illegal/unauthorized sources gets the same legal treatment as downloading in every national law, as in both cases the user makes a permanent copy of the work. In sum, the majority of national laws consider it a direct infringement of the reproduction right.

However, the novelty of the use and the absence of case law make this assessment uncertain. A particularly unclear issue is whether this activity qualifies as a violation of anti-circumvention provisions on TPMs. This would likely require qualification of the stream itself as an effective copy-control technological measure in legal terms, which is dubious. In this regard, at least some national laws require a subjective element (knowledge, awareness, intent) in connection with TPM circumvention (e.g. France, Germany, and Japan).

Finally, in many instances stream-ripping occurs from platforms authorized by copyright holders or shielded by safe harbors, such as Netflix or YouTube. In these cases, the source itself is not illegal but rather an authorized online service provider. In some cases, the act of ripping the stream is a breach of the service provider’s terms of service, a consideration that may affect the legal status of the act, e.g. by causing the ripped copy to not meet the requirement that it originates from a lawful or authorized

source (see *supra* on *downloading*, especially in the EU). However, in the absence of clear guidance from statute or case law in this respect, the legal status of this activity remains uncertain.

Uploading: Uploading content to a publicly accessible website without permission of the copyright holder is either universally qualified as a direct infringement of the reproduction *and* communication/making available to the public rights (France, Poland, Sweden, arguably the UK, and Indonesia), or solely of the communication to the public right or a national equivalent (the remaining national laws). Only two national laws contain exceptions that may apply to this activity. Under Canadian law, it may be lawful to upload works (often not in full) to an online platform under the exception for user-generated content, as well as the limited *fair dealing rights* for purposes of research, education, parody, or satire. In Hong Kong, the act may in certain cases benefit from a *fair dealing defense*.

Hyperlinking: The legal status of hyperlinking is highly controversial in EU law, following judgments from the CJEU from *Svensson* to *Ziggo*. After the landmark *GS Media* decision, posting links to unauthorized content is subject to a knowledge test connected to a for-profit condition: in simple terms, the for-profit nature/intent of the linker triggers a presumption of knowledge of the unauthorized nature of the content, which if not rebutted leads to a finding of direct infringement of the right of communication to the public. As a rule, national laws in the EU follow this approach, despite its inherent uncertainty.¹ Consequently, posting hyperlinks of this type is infringing, as no exception applies. The introduction of a knowledge test in the assessment of primary liability for this exclusive right is a departure from the strict liability paradigm in copyright law.

The situation differs outside Europe. First, there is little case law on this type of acts, leading to uncertainty in their legal qualification. Second, some national laws qualify the act as direct infringement of the right of communication to the public, without the need to assess subjective elements (Thailand, Hong Kong). Third, other national laws deal with this issue within the realm of intermediary or secondary liability, as in the case of Canada, Brazil (joint liability or solidarity, requiring commerciality of the link), or Japan (tort of facilitating the illegal public transmission of works). Finally, in Indonesia, it appears that posting hyperlinks does not give rise to liability for copyright infringement.

Sale of kodi boxes. In the EU, *Filmspeler* raised the possibility that the sale of kodi boxes including by default add-ons that link to works available online without the permission of the copyright holder constitutes direct infringement of the right of communication to the public. The CJEU applied the *GS Media* knowledge test to this case, leading to a finding of direct infringement. Before the judgment, this activity was dealt with in the realm of intermediary liability (e.g. in Poland and Germany). After the judgment, most experts consider this to be a case of primary liability, subject to a knowledge test as described above. Since no exception applies, the act is a direct infringement of the right of communication to the public.

Outside the EU, there is nearly no case law on the topic, making for an uncertain legal qualification of this act. Based on broadly worded economic rights in national law, the Brazilian expert notes that this would probably (more likely than not) qualify as direct infringement. The situation is uncertain in Canadian law: despite the grant of interlocutory injunctions in two cases (against the sale of set-top boxes and a website providing add-ons for Kodi boxes), the legality of this activity is yet to be assessed in a pending case.² The situation also diverges in Asian countries. In Thailand, this activity could be covered by the right of communication to the public, subject to requirements of knowledge (or awareness) and commerciality. Conversely, Japanese and Hong Kong law would probably deal with this activity under the heading of intermediary/secondary/contributory liability and/or

¹ But see a recent decision from the German Federal Court ruling that in the knowledge presumption does not apply in case of search engines. German Federal Court: BGH, Urt. V. 21.9.2018 – I ZR 11/16.

² Report Canada, citing *Bell Canada v. 1326030 Ontario Inc. [iTVBox.net]*.

infringement by authorization. In Indonesia, the expert merely clarified that the act does not qualify as direct infringement of copyright.

Others types of unauthorized use. The national experts did not report any significant additional types of unauthorized online use of copyright-protected content not included in the activities described above.

Areas of legal uncertainty regarding primary liability

The analysis of primary liability in national laws uncovers three main areas of legal uncertainty: absence of case law on some activities; experiential use (passive streaming); referential or mediated use (hyperlinking and sale of kodi boxes).

First, the absence of case law on many types of acts makes it hard to state with certainty whether they infringe copyright in some national laws. This is particularly true for acts like stream-ripping, passive streaming, hyperlinking and the sale of kodi boxes with unauthorized add-ons. In the EU, some of this judicial scarcity can be overcome to a certain degree by relying on the interpretative activity of the CJEU. In other jurisdictions, especially in Brazil and the Asian countries, it is only possible to rely on probability assessments by national experts. Therefore, some caution must be exercised before drawing sweeping judgments on the basis of the questionnaires.

Second, the legal qualification of passive streaming as a copyright-relevant act is unclear. In the EU, the issue appears to be settled after *Filmsteper*. However, outside Europe, it is noteworthy that some national laws do not consider this activity to merit copyright protection. This is grounded on the notion that that passive streaming is experiential in nature, akin to the offline equivalent of reading a book or viewing a TV series. As such, streaming would not constitute a *use* of copyright in the legal sense.

Third, there is uncertainty in what we term “referential” or “mediated” use. This refers to types of acts like hyperlinking and the sale of kodi boxes (with pre-installed add-ons), that are in some countries *probably* governed by the right of communication to the public under a strict liability regime (Thailand and Hong Kong), in EU national laws governed by the same right but subject to a knowledge test stemming from CJEU case law, in yet another set of laws governed by intermediary liability regimes (Canada, Brazil and Japan), and in one country apparently not giving rise to liability for copyright infringement (Indonesia). Our main observation in this respect is that for these acts there is a blurring of the lines between primary and secondary liability, with a significant degree of uncertainty as to the application of subjective elements in the assessment of the exclusive right of communication to the public.

Knowledge, commerciality and content type

As a rule, there appear to be no noteworthy differences for the assessment of primary liability depending on the type of content at issue, namely music, films and TV series, books, or video games. To be sure, the legal qualification of video games in national law as an independent work and/or as software was not clear in all questionnaires. However, this potential difference does not appear to affect the main conclusions regarding liability for the acts described above.

Regarding knowledge and commerciality, the main points to emphasize are those addressed above under the heading “areas of legal uncertainty”. In sum, other than the consideration of knowledge in the context of the legal qualification of downloading in Japanese law, the majority of acts described – from downloading to uploading – are strict liability torts. The situation differs when assessing the right of communication to the public in EU countries, and its application to hyperlinking and the sale of kodi boxes. In those cases, the subjective element of knowledge plays a central role in the legal qualification of the act. Furthermore, when assessing knowledge in that context, the CJEU has devised a rebuttable presumption that relies on the for-profit nature, character and/or intent of the linker, the

precise contours of which are still in flux. Thus, in this context, the commercial nature or intent of the act plays an important role in the legal assessment of primary liability.

For a Summary Table of the online acts qualified as copyright infringement across different national countries, please refer to ANNEX 3: Summary Tables Question 3 – online acts qualified as copyright infringement.

Intermediary or secondary liability: notion of intermediary and safe harbors

In the EU, all national laws have implemented the ECD's safe harbors and no monitoring obligation, as well as related provisions. (The relevant exception is Poland, which has not implemented Article 8(3) of the InfoSoc Directive on injunctions against intermediaries.) Most laws fail to provide copyright-specific notions of "intermediary", advancing instead broader notions of intermediary or service provider in civil law or in national e-commerce legislation. Due to the implementation of the ECD, all national laws contain a definition of "information society service provider" or the like.

The laws analyzed do not appear to contain positive rules determining the liability of Internet intermediaries, but rather a partial regulation of the same through safe harbors that provide liability exemptions or immunities (for damages) to at least three types of intermediary services – mere conduit, caching, and hosting – in terms identical to the directive, as interpreted by the CJEU.

Despite that, there are some noteworthy idiosyncrasies in national laws. For example, Spanish law contains a separate safe harbor for search engines and hyperlinks (which other laws place under the hosting exemption), while Dutch law provides a safe harbor from criminal copyright liability identical to those existing for civil liability. Swedish law, for its part, contains not only a "social benefit" exception for contributory criminal liability, but also a criminal liability provision aimed at service providers that transfer or store information for another; the latter has been used to exclude applicability of safe harbors to the operators of *The Pirate Bay* and convict them of criminal secondary liability. Finally, UK law clarifies the applicability of safe harbors not only for damages, but also for any other pecuniary remedy or any criminal sanctions.

The most controversial safe harbor is that of hosting and its application to large scale user-upload websites, such as YouTube and Daily Motion (as exemplified by judgments in France, Germany, and Spain). As a rule, the hosting safe harbor is tied to requirements of actual knowledge and/or awareness of the illegality of the content hosted, coupled with an obligation remove and/or disable the content hosted upon acquiring knowledge.

In most cases, actual knowledge results from notice of the infringement sent by the copyright holder or his representative, containing a number of legally defined elements (e.g. information about applicant, description of facts and URL, legal basis, etc.). Reception of a valid notice leads to an obligation of prompt takedown by the intermediary.

A more elaborate private notice-and-takedown (NTD) system is set up in the Netherlands. Based on the implementation of the directive in its Civil Code, several Dutch intermediaries adopted a Code of Conduct setting out voluntary NTD procedures for copyright infringing content. Notably, only two other Codes of Conduct were mentioned by national experts in their responses, both of them in the UK. The first is the Voluntary Copyright Alert Programme (VCAP), which forms part of the industry-led scheme Creative Content UK; this is discussed below in the context of *administrative enforcement measures*. The second is the Voluntary Code of Practice on Search and Copyright agreed in early 2017 by leading search engines, entertainment trade bodies, and music industry body BPI, in a deal brokered by the UK Intellectual Property Office. Under the Code, search engines commit to the removal of links to websites that have been repeatedly served with copyright infringement notices from the first page of their search results, with the aim of preventing UK internet users from

downloading and streaming protected content illegally. These commitments include specific targets for reducing the visibility of infringing content in search results.

It is important to note that safe harbors set out specific liability exemptions but do not establish the conditions under which intermediaries are liable for copyright infringement by third parties using their services. Most national laws determine such liability through the application of general tort law and doctrines of contributory infringement. Due to the specificities of online copyright infringement, this has led to the development of specific torts for Internet intermediaries. In Germany, courts usually rely and develop the civil law tort of “interferer liability” (*Störerhaftung*). An interferer is a person who has willfully made a causal contribution to the direct copyright infringement by a third party. Such an interferer can be held liable for injunctive relief (not damages) if it has violated a reasonable duty of care to prevent the direct infringement at stake. These rules articulate with safe harbors insofar as compliance with the latter is considered when assessing if the intermediary has violated a reasonable duty of care. Spanish law, differently, has implemented a tort of indirect liability that strongly resembles a transplant from judge-made doctrines in US law, as it includes identical formulations on contributory infringement, inducement, and vicarious liability.

The legal landscape of intermediary liability **outside the EU** is irregular. In Brazil, the Copyright Act does not define intermediaries or include safe harbors. A different piece of legislation, the Internet Civil Act (*Marco Civil*) does include such provisions, but it expressly excludes its application to copyright. This has led courts to deal with intermediary liability by combining provisions from the Copyright Act, the Civil Code and the Consumer Rights Code. In doing so, the Superior Court of Justice has developed a secondary liability (“subsidiary responsibility”) regime for hosting providers relying on tort law. This is in essence a NTD regime where knowledge is obtained by a sufficiently complete private notice, which gives rise to an obligation to promptly remove content on a temporary basis. The provider must then assess the legality of the content and may re-upload the content if it considers it lawful. Different factors must be taken into account when assessing the liability of providers in this context.

Canadian law is different insofar as it contains a rich mix of intermediary liability provisions. First, it provides a general safe harbor for intermediaries, according to which the mere supply of a (broadly construed) “means of telecommunications” does not give rise to liability for the provider. This is complemented by specific safe harbors for the traditional types of intermediary services, namely network services (mere conduit or access), incidental acts (caching), and hosting, as well as for “information location tools”. The combined application of these provisions, as interpreted by the courts, exempts from civil liability a broad range of intermediaries, including search engines.

The application of safe harbors is subject to specific conditions for each category of services (e.g. neutrality and knowledge), but also to a general condition, namely that the act at stake does not infringe upon a general “enabler liability” provision. This provision has also the function of positively defining the instances in which an intermediary is liable, i.e. when its service is used primarily for the purpose of enabling copyright infringement and an actual infringement occurs as a result of the use of the service. Note, however, that there is no case law on this provision yet.

Canadian law also includes two further idiosyncrasies. First, it has instituted a “notice-and-notice” system, under which an ISP does not have to takedown content or disclose personal data, but merely relay the notice of infringement to its subscriber linked to the IP address. The non-compliant ISP is only subject to capped statutory damages. Finally, the Copyright Act provides for a user-generated content exception. Where the exception applies to uploading by end-users, the hosting platform in question will not be liable for hosting that content.

Further different regimes exist in Asia. In Hong Kong, for example, there are no safe harbors for intermediaries. Their liability can be established under two headings – infringement by authorization and contributory infringement as a common law tort –, which both imply case sensitive inquiries as to issues like content removal and obligations of intermediaries.

In Indonesia, there are also no specific safe harbors. Intermediaries are subject to a duty of care principle stemming from the Civil Code as well as to specific obligations specified in different Circular Letters from competent Ministries. These include providing reporting means for infringing content they host and removal or blocking of content upon acquiring knowledge thereof.

Japanese law is unclear on the criteria for definition of intermediary liability but does contain safe harbors for damages from infringement caused by information distribution. These are conditional upon the technical possibility of preventing such distribution and knowledge or awareness of the infringing act or the possibility of its occurrence. To avoid liability, the ISP must act upon that knowledge and remove the content.

Finally, the law of Thailand provides for a safe harbor (regarding damages) for intermediaries that are neutral towards the infringing content and comply with a judicial order against the same.

Areas of legal uncertainty regarding intermediary or secondary liability

In the EU, there is uncertainty in the majority of the Member States as a result of CJEU case law on the right of communication to the public and on the safe harbors in the ECD. On the one hand, the broad interpretation of the right and the introduction of subjective elements in its assessment extended its application to the activities of certain online platforms, in particular those hosting content. On the other hand, the CJEU has clarified that only predominantly “neutral” (but not necessarily passive) intermediaries may benefit from safe harbors. Further uncertainty arises from the difficulty in assessing the “actual knowledge” requirement for hosting platforms, as well in delineating what constitute admissible “specific” monitoring obligations for intermediaries. Thus, in this context, it remains unclear where to draw the line between primary liability and the safe harbor provision for hosting platforms in the ECD. (This mirrors a main topic of controversy at EU level with the current proposal for Article 13 of the draft Directive on Copyright in the Digital Single Market.³)

Some of these challenges are echoed in national laws. For instance, German law struggles in differentiating when hybrid service providers (e.g. YouTube) use own information/content – in which case they are primarily liable – from when they use external or third party information content, in which case they may benefit from safe harbors. In Spain, the articulation of the relatively new provisions on indirect liability with safe harbors is yet to be defined. Finally, in Sweden there is the expectation that some types of acts currently dealt with as intermediary liability are recast as instances of primary liability, with consequences for the types of remedies available against online platforms.

Outside Europe, there are also certain areas of legal uncertainty, but not to the same extent as in the EU. In Brazil, for example, there is uncertainty on how to establish liability of ISPs in the context of the evolving judge-made doctrine of “subsidiary responsibility” described above. In Canada, the main uncertainty regards the absence of case law on the aforementioned provision on “enabler liability”, which operates also as a condition for the application of safe harbors.

In Hong Kong, the extent of involvement required to establish the liability of intermediaries remains uncertain, as the potentially applicable doctrines – infringement by authorization and contributory infringement as a common law tort – are heavily case sensitive and have not been sufficiently interpreted by the courts. In Indonesia, any uncertainty would probably relate to the case-by-case application of the duty of care principle to online intermediaries. In Japan, there are doubts surrounding the legal qualification of video sharing platforms as direct infringers of ISPs benefiting from safe harbors. Finally, in Thailand, the uncertainty relates to whether existing safe harbors can shield ISPs from liability arising out of criminal copyright infringement.

³ COM (2016)593 final, Art. 13 on “Use of protected content by information society service providers storing and giving access to large amounts of works and other subject-matter uploaded by their users”.

Treatment of copyright infringement by minors

In the EU, civil liability of minors for copyright infringement is typically not distinguished from that of adults. As a rule, parents, guardians or the people defined by law as having supervisory power or duty over minors (jointly “parents”) are liable for damages as a result of the latter’s infringing acts. The exception to this rule is Swedish law, which does not attribute such liability to parents.

The general principle can apply irrespective of the minor’s age (France and Spain) or vary according to that age. Thus, in some countries, minors can only be liable as from a certain age, e.g. seven years of age in Germany and thirteen years of age in Poland. In other laws, the attribution mechanism may vary according to age and other factors. For instance, in the Netherlands, parents are only fully liable until the minor is fourteen years old. Between fourteen and fifteen, parents may be exempt from liability if they cannot be blamed for failing to prevent the act; the minors, on the other hand, may be solely liable if they commit a “tortious act”. This is illustrated by the case of a fifteen year old boy managing a website that published without permission or attribution two photos of Johan Crujff (a famous Dutch football player): the minor was ultimately considered liable but his parents not. Another noteworthy judgment in this respect comes from the German Federal Supreme Court in the 2012 *Morpheus* decision, where it stated that although parents must explain copyright law to their children, they have no obligation to monitor their Internet use.

In most remaining countries outside Europe (Brazil, Canada, Hong Kong, Indonesia, Japan, and Thailand), the law makes no significant distinction between minors and adults for purposes of civil copyright infringement. However, the laws of Brazil and Thailand make criminal liability depend on the minor’s age. (In Brazil, a person is a minor until eighteen years of age, whereas in Thailand that age is twenty.)

ENFORCEMENT MEASURES, PROCEDURES, REMEDIES AND SANCTIONS

This part of the study deals with public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (like warnings), or criminal (such as prison sentences). Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries.

Enforcement measures against users

Civil enforcement measures

At EU level, civil measures are harmonized in the Enforcement Directive, and include different types of injunctive relief and damages calculated according to the directive (as a rule, punitive or exemplary damages are not available). All member states have implemented the directive with varying degrees of detail, and largely follow its regime. Some details are worth pointing out.

German law includes provisions that incentivize parties to settle claims out of court, namely detailed requirements for notifications to alleged direct and indirect infringers (to “cease and desist”) prior to instituting judicial proceedings. Dutch law allows for ex parte injunctions in the context of preliminary relief proceedings, subject to a showing of a risk of irreparable damage. Spanish law contains injunctions under the format of “restraining orders” specifically designed for the online environment, including measures to suspend Internet access of infringers, block access to or remove infringing content from websites, as well as injunctions to require personal data of the infringer from ISPs in “special cases”.

UK law does not entitle the copyright holder to damages if, at the time of infringement, the defendant did not know or had no reason to believe that copyright subsisted in the work to which the action relates. However, additional damages may be available taking into account the flagrancy of the infringement or the profits made by the infringer. An account for profits is available as an alternative

for damages. As regards injunctions, UK law has developed a “search order” (formerly the “Anton Pillar order”) to allow the preservation of evidence prior to trial in copyright infringement cases, which can be combined with a “freezing” or “asset preservation” order for the retention of property pending litigation. (Specific injunctions for disclosure of personal data, such as the Norwich Pharmacal Order, are detailed further below.)

Outside the EU, Brazilian law provides for injunctions and damages for copyright infringement. However, since the law is outdated regarding online use, the application of such measures must in some instances be done through analogy. Still, there is sufficient flexibility in the law to encompass injunctions and coercive fines against individuals or platforms that disseminate works online. Furthermore, the provisions on damages – even where they refer to offline copies – can arguably accommodate the specificities of online infringement. Finally, a recent trend in the case law points towards a consideration of ISPs as jointly liable for copyright infringement where they fail to takedown content subsequent to an adequate (private) notice.

Canadian law imposes liability on users for copyright infringement and circumvention of TPMs. Regarding infringement: copyright holders are entitled to injunctions, damages and accounts. Statutory damages for commercial and non-commercial infringements are available as an alternative to actual damages. The regime is similar for TPM circumvention, with the exception that no statutory damages are available against individuals who circumvent TPMs for their own private purposes.

The laws of Hong Kong, Indonesia, Japan, and Thailand all provide for injunctions and damages against direct infringers. In addition, the law of Hong Kong provides interesting parallels with UK law: it contains a specific injunction for disclosure of personal information (Norwich Pharmacal Order); it does not provide for damages against innocent infringers; it allows additional damages in certain cases, depending on factors like the “flagrancy of the infringement” or the profits made by the infringer, but considers in addition “completeness, accuracy and reliability of the defendant's business accounts and records.” Another parallel with UK law is found in Indonesia, which law provides for “Anton Pillar Orders”.

Administrative enforcement measures

Administrative enforcement measures against direct *online* copyright infringement by users only exist in France, the UK, Indonesia, and Thailand. In addition, Spanish law contains a special administrative procedure directed at ISP that can be considered to apply both to “users” and “intermediaries”, depending on how these concepts are defined.

With relevance to online infringement, French law includes a graduated response system that is of mixed nature, administrative and criminal. The system, which has gone through different iterations, is managed by an administrative authority (HADOPI), and works as follows. Individual Internet users have an obligation to ensure that their connections are not used to infringe copyright. After a 2013 amendment, the penalty for violating this obligation is no longer Internet disconnection but, instead, fines up to €1.5 thousand. This sanction can only be levied if certain conditions are met; notably, not having a secure Internet connection may not allow the subscriber to avoid sanctions.

In the UK, the Digital Economy Act 2010 (DEA 2010) included a graduated response system for the online enforcement of copyright, with similarities to the first iteration of its French counterpart (i.e. including Internet disconnection as a sanction). However, this controversial system was never adopted. Instead, in 2014, the UK government promoted the adoption of an industry-led scheme called Creative Content UK, adopted by the UK’s creative industries and ISPs. One major element of this scheme was the aforementioned Voluntary Copyright Alert Programme (VCAP), a programme of email alerts sent by ISPs to residential broadband subscribers whose accounts are used to infringe copyright via peer-to-peer (**P2P**) file-sharing. The VCAP involves agents of copyright owners sending evidence of copyright infringement to ISPs, which then send letters or alerts to infringing customers with the intent to discourage infringement. A maximum of four letters with language escalating in

severity can be sent to a single IP address. No sanctions are admitted under the VCAP, but copyright holders are free to pursue legal action against the individuals. The first letters were sent to subscribers in early 2017.

Indonesian law contains a Joint Regulation of two Ministries from 2015, based on a provision in the Copyright Act. This regulation provides for a procedure for complaints related to online copyright infringement reported to either of the two Ministries mentioned, directly or through an electronic system in the website of the competent authority. Complaints can be submitted by copyright holders, licensees or CMOs, and are verified by a team at one of the Ministries, who issues recommendations on applicable measures. Decisions can be made to partly or entirely block access to infringing content, and there is a database of blocked sites/users. In addition, a Circular Letter from a Ministry imposes on user-generated content platform providers an obligation to provide a reporting instrument for complaints regarding inter alia copyright infringing content they host. If sufficient evidence is provided with the notice/complaint, platform providers must take necessary action to remove the content or block access thereto.

The law of Thailand, in particular the Computer-Related Crimes Act, provides for an administrative enforcement measure for copyright infringement that constitutes a crime. This measure allows officials with approval from the Minister to file petitions for writs to stop dissemination of information, or to order the deletion of data from systems where inter alia the information or data in question qualifies as criminal copyright infringement. If the copyright infringement “bears characteristics which are contrary to peace and order or good morals”, a separate procedure applies, involving the intervention of a “Computer Data Screening Committee” prior to the Minister’s approval. In both cases, this power is broad in scope, allowing competent/authorized officers to compel the removal or suppression in question, or to carry it out by themselves. Users that do not comply with the court order are subject to multiple fines.

Finally, Spanish law introduced in 2011 a special administrative injunction procedure by the Intellectual Property Commission or CPI (sec. 2) against infringements done for commercial purposes by ISP. The procedure, reinforced and enlarged in 2004, may be understood as applying both to users and intermediaries. This is because it covers not only categories of intermediaries that traditionally benefit from safe harbours (e.g. pure hosting) but also websites that may be qualified as directly infringing copyright, depending on the specific case. The latter include user-generated content websites and those providing links to infringing contents, which may for example directly infringe upon the right of communication to the public. Where the procedure applies the latter type of website, it may be considered as targeting also “users” (*lato sensu*). Measures available under this procedure include the suspension of the Internet service provided to the infringer, blocking and removing infringing contents, and publication of notices regarding the infringement. For further details on the procedure and its application to intermediaries, see the comments below on administrative enforcement measures against intermediaries.

Criminal enforcement measures

There is no harmonization of criminal measures against copyright infringement in the EU. Most member states criminalize intentional acts of direct copyright infringement and subject them to varying sanctions, ranging from fines to prison terms, and including seizure of infringing material and publication of the sentence. Offences are usually aggravated if they occur on a commercial scale or with a for-profit aim. Among the crimes listed is the manufacture and distribution of TPM circumventing devices.

Whereas in countries like Germany these provisions are irrelevant in practice, they play a more prominent role in France and Spain, to name two examples. In France, for instance, in addition to the typical criminal provisions, for offences committed using an online service courts can order the additional penalty of suspension of Internet access for a maximum of one year, during which period the person is prohibited from entering into another contract for the same service with any operator.

The termination is notified by the court to the HADOPI, who in turn notifies the ISP to carry it out under the penalty of a fine. Spanish law, for its part, has been amended in 2015 with the aim of extending the scope of criminal copyright sanctions to users of P2P services, a change that appears to be nudging the courts to increasingly condemn these types of users (as well as the respective platform operators). In Sweden, criminal provisions have been used to target a user of a file-sharing website for contributory criminal liability.

Two interesting idiosyncrasies should be noted. First, Swedish law does not criminalize the reproduction of computer programs – and by extension video games – for personal non-commercial use on condition that the original copy of the computer program that was reproduced is not being used for commercial purposes or in the public sector. Second, Polish law includes special criminal offences that only apply to software and works including software, such as video games.

The general framework of criminal measures in the American and Asian countries is similar to that of EU member states. One relevant difference is found in Brazilian law, which does not criminalize acts covered by an exception or limitation or the making of single copies of copyright-protected content for private and non-commercial aims (e.g. in the context of downloading or stream-ripping).

Enforcement measures against intermediaries

The aim of enforcement measures against intermediaries is for them to end or prevent infringement by third party users of their services. Examples of such measures include: suspension from the Internet of the infringer; measures to identify the infringer; the monitoring or filtering of content; the blocking or removing of infringing content, including in the context of NTD procedures; warning systems; obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service; graduated response systems.

Civil enforcement measures

Under EU law, intermediaries that qualify for the safe harbors in the ECD are not liable for damages but only for injunctions – pursuant to Article 8(3) of the InfoSoc Directive – and duties of care, as permitted by the ECD and further established in national law. In all cases, measures must not conflict with the general prohibition against monitoring (under the national equivalent to Article 15 ECD) and must strike a fair balance between competing fundamental rights in line with CJEU case law.

Under this heading, all member states contain different flavors of measures. It is worth providing some examples of those that are most unique to online enforcement.

- In France, if a computer program is mainly used for unlawfully making available protected content (e.g. P2P software), a judicial order may be issued to take all necessary measures to protect the right in question, which may include certain filtering mechanisms. In addition, a court may also order an ISP whose services are used for copyright infringement to implement measures to prevent or to block the infringement acts (e.g. removal of suggestions from a search engine service).
- In Germany, the tort of “interferer liability” allows for injunctions against intermediaries that violate reasonable duties of care to prevent such direct infringements. These include removing infringing content upon notice from copyright holders, and taking reasonable measures such as filtering to prevent further comparable infringements in the future. Information injunctions are also available against intermediaries.
- Dutch law contains several measures potentially applicable to intermediaries, such as NTD (pursuant to the aforementioned voluntary code of conduct adopted by Dutch intermediaries), injunctions for website blocking (of domain names and IP addresses), and measures for the identification of infringers.
- In Poland, enforcement measures against intermediaries are difficult to apply, especially as national law has not implemented Article 8(3) of the InfoSoc Directive.

- Spanish law allows for injunctions and precautionary measures against intermediaries irrespective of applicable safe harbors. In this context, an ISP may be ordered to suspend the Internet service provided to the infringer, block and/or remove infringing content hosted in its server, and publish notices regarding the infringement. An ISP may be ordered to provide information to identify the infringers in *civil* proceedings since 2014.
- Swedish law deviates from Article 8(3) of the InfoSoc Directive insofar as it only allows enforcement measures against intermediaries if they are at least secondarily liable for infringement (with the exception of information injunctions). In addition, intermediaries may be subject to general injunctions, including interim injunctions and blocking orders, with the expert noting a recent shift in national law towards broadening the scope of secondary liability.
- In the UK, Article 8(3) of the InfoSoc Directive was implemented in Section 97A CDPA, which allows injunctions against ISPs, subject to certain conditions. Most of the case law on this provision concerns blocking injunctions. In addition, intermediaries are also subject to *Norwich Pharmacal* orders (**NPO**), i.e. a form of disclosure order that amounts to an information injunction.

Outside Europe, Brazilian law does not specify enforcement measures against intermediaries. As noted above, this led to the Superior Court of Justice developing a secondary liability or “subsidiary responsibility” regime for hosting providers on the basis of tort law. Failure by ISPs to meet the conditions of this regime subjects them to contributory liability and remedies like injunctions and damages.

As described above, Canadian law contains generous safe harbors for intermediaries and a notice-and-notice regime aimed at discouraging online copyright infringement. Under this regime, a claimant’s only remedy against an ISP who fails to perform its obligations is statutory damages capped at \$10 thousand. The law further includes as an exception to safe harbors the aforementioned provision on “enabler liability”. The provision has yet to be interpreted by the courts but could apply to platforms like *The Pirate Bay* or *Popcorn Time*. Canadian law also includes a somewhat similar rule prohibiting the provision of services or manufacturing technology primarily for the purposes of facilitating the circumvention of TPMs. Finally, copyright holders have the possibility to obtain information injunctions against ISPs under the form of Norwich Orders.

Under Hong Kong law, intermediaries may be liable for infringement by authorisation or contributory infringement. If found liable, they are subject to similar civil remedies as direct infringers, namely injunctions and takedown orders, damages, and account of profits. Injunctions may include: takedown orders against forums; website blocking orders against ISPs; and de-indexing orders against indexing and bookmarking sites, including search engines. The law of Indonesia does not contain specific civil enforcement measures against online intermediaries. However, since civil liability of intermediaries is based on a duty of care principle, a finding of liability will lead to the application of the same civil remedies as for direct infringers.

Under Japanese law, it is unclear whether intermediaries are subject to injunctions similar to those available under Article 8(3) of the InfoSoc Directive, despite a specific instance (*TV Break Case*) where a video-sharing platform was subject to an injunction for direct infringement. An intermediary will be subject to the remedy of damages available in the Civil Code if considered a joint tortfeasor. In addition, the ISP Liability Limitation Act allows for a specific information injunction against ISPs. Finally, the law of Thailand allows for intermediaries to be subject to remedies of damages and injunctions if they are negligent and cause damages to right holders.

Administrative enforcement measures

Most national laws do not contain administrative measures specifically targeting (online) intermediaries. To the extent intermediaries qualify as users due to the nature of their activities, they will be subject to the administrative measures available against direct infringers. The exceptions to this are Spain, the UK, Indonesia, and Thailand.

In Spain, as noted above, there is since 2011 a specific injunction procedure with the Intellectual Property Commission or CPI (sec. 2) against ISPs whose services may inter alia be used by third parties to infringe copyright for commercial purposes. The procedure applies to two types of infringement by ISPs that can be simply defined as (1) significant infringement (e.g. providing access to unauthorized works on a large-scale), and (2) facilitation of infringement (e.g. providing access to and organizing lists of links to unauthorized content). If the ISP fails to withdraw content or cease the infringement, this broad injunction allows the CPI (sec. 2) to order a range of measures, subject to payment of fines. These measures include the suspension of the service provided to the infringer, the blocking and removing of infringing contents or domain names, suspension of advertisement on the infringing site, and the publication of notices regarding infringement. Rulings of the CPI (sec. 2) require prior judicial approval by an administrative court. Based on the data available on these measures and reported by the expert, it is unclear if this injunctive measure is effective.

In the UK, the described VCAP system is also relevant for intermediaries insofar as their services are used to send notices to end-users.

In Indonesia, the aforementioned Joint Regulation affords ISPs some discretion on how to deal with infringing content or activities carried out by third parties using their services. The intermediary will first send the user a warning letter to cease the infringement and/or terminate its contract with the user, leading to the blocking or deletion of the allegedly infringing content. Furthermore, it is possible that the user's Internet access is suspended pending the finalization of the process for producing evidence of the infringement by the Ministry of Communication and Information.

Finally, in Thailand, two administrative measures are available against intermediaries: (1) the Copyright Act allows for a court order against an ISP for the removal of infringing content from its system; (2) the Computer-Related Crime Act provides for an administrative enforcement measure in case of copyright infringement that constitutes a crime, aimed at the suppression of dissemination or removal of computer data which infringes copyright and constitutes a criminal offence. The ISP that disregards the first type of Court order faces no penalty but is subject to a subsequent *civil* lawsuit where this conduct may be relevant. Failure to comply with the second order subjects the provider to steep fines.

Criminal enforcement measures

Most national laws do not contain criminal measures specifically targeting (online) intermediaries. To the extent intermediaries commit, or are involved in (by assisting or inducing others), any of the crimes of copyright infringement defined in national law, they are subject to the criminal measures mentioned above for users. Apart from that, it is worth to briefly mention the laws of Spain and Japan.

In 2015, Spanish law introduced a new crime tailored for websites that offer links to infringing contents (e.g. on P2P and other platforms) and regardless of whether their activities are themselves infringing. The crime does not apply to "neutral" search engines or to ISPs that only "occasionally link to third party infringing contents".

Regarding the situation in Japan, other than the measures applicable to accessories to a crime in the Japanese Penal Code, the national expert makes reference to a court case concerning the "Winny" file sharing software. In this case, after the Kyoto District court convicted a person who released the software of a crime of inducing third party copyright infringement, both the Osaka High Court and later the Supreme Court denied the crime on the ground that the accused lacked intent to be an accessory to the crime of copyright infringement.

Differences in public vs. private enforcement per content type

In most national laws no significant differences were noted in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games). Only in Poland, Spain and Brazil minor differences were noted, which however did not translate into significant differences in enforcement practices. This is for example the case of the consideration of video games as software in Poland, with the effect that this type of content is subject to special rules regarding certain criminal offences.

Disclosure of personal data in the context of enforcement

In the EU, Article 8 of the Enforcement Directive provides for a right to information. Furthermore, the CJEU has interpreted Article 8 of the InfoSoc Directive in *Promusicae* as not imposing nor preventing member states from mandating ISPs to disclose personal data of their subscribers in the context of copyright infringement proceedings. Against this background, most European national laws contain a legal obligation for intermediaries to disclose the personal data of individuals involved in copyright infringement. The obligation is subject to conditions, like the need for the copyright holder to meet requirements to evidence the infringement (such as showing of manifest infringement) and a judicial order. The information typically requested is that necessary to pursue an infringement lawsuit against the user, and generally includes his account information, other identification details (name, address, place of residence), payment details, and IP address. Some additional details and deviations should be noted.

- In the Netherlands, the Supreme Court has held that online intermediaries may also be obliged to disclose personal data of individuals involved in copyright infringing activities to right holders on the basis of a general duty of care resulting from Article 6:162 of the Dutch Civil Code. On the basis of such duty of care, intermediaries may be compelled to make their own independent assessment and hand over personal data to right holders without a court order being present. If intermediaries fail to disclose personal data they may be acting in violation of said duty.
- Polish law provides no legal basis for an obligation to disclose personal data of individuals involved in copyright infringing activities. However, right holders may obtain such information through other legal provisions.
- Swedish law goes beyond Article 8 of the Enforcement Directive and allows copyright holders to apply for an information injunction without the need for an infringement case pending before the court.
- UK law, as mentioned, contains a specific information injunction under the form of an NPO. This is a form of disclosure order, made under the equitable jurisdiction of the court, used in cases where the identity of the wrongdoer is unknown but it is possible to identify a third party who has this information. NPOs have been used to identify end-users in the context of P2P litigation.

Outside the EU, countries like Canada and Hong Kong include variations of NPOs to compel the disclosure of personal data of an alleged infringer by the online intermediary, pursuant to certain requirements, including a court order. With minor differences, the situation appears to be the same in Japan and Thailand (although in the latter case on the basis of a Constitutional provision). Brazilian law does not include a legal obligation to disclose personal data in the context of copyright infringement, but copyright holders may nonetheless obtain such data through strategic litigation, leveraging the legal obligation of ISPs to retain personal data under the Internet Civil Act. Finally, the law of Indonesia lacks any legal obligation or case law in this respect, although the expert considers that the disclosure of such data could be possible in the context of a copyright infringement lawsuit.

Entitlement to apply for enforcement measures⁴

In the EU, the Enforcement Directive contains rules on standing to sue. According to these, the persons entitled to seek *civil* enforcement measures are the right holders, authorized users (e.g.

⁴ Reference is made in this section of the summary only to *civil* enforcement measures.

licensees), authorized CMOs, and authorized professional defense bodies. The directive further establishes a presumption of authorship and ownership of copyright in favor of authors and related right holders if their name appears on the work or other subject matter “in the usual manner”. National laws of member states are for the most part consistent with the directive, with some differences regarding the conditions under which licensees and professional defense bodies are entitled to apply for measures. For instance, non-exclusive licensees do not have such entitlement in Germany, Poland and Spain.

The situation is similar in other countries. In Brazil copyright holders, assignees and licensees are entitled to apply for enforcement measures. CMOs can do so as well, provided the infringement falls within their representation powers. Under Canadian law, the copyright owner or any person deriving any right, title or interest by assignment from the owner are entitled to apply for measures. This entitlement extends to exclusive licensees but not to non-exclusive licensees and sole licensees. CMOs have standing to enforce payment of royalties under an approved tariff or agreement.

Hong Kong law allows the copyright holder and the assignee to apply for enforcement measures. An *equitable* assignee must join the copyright holder before final relief can be obtained, and an exclusive licensee is entitled to apply after joinder with the copyright holder. In Indonesia, the copyright holder and/or exclusive licensee are entitled to apply for measures. Under Japanese law, the copyright holder may apply for enforcement measures and there is strong support for the possibility of the exclusive licensee being also entitled to apply subject to certain conditions. Finally, in Thailand, copyright holders and authorized persons (such as licensees and CMOs) are entitled to apply for enforcement measures.

Most used and effective enforcement measures

To conclude, experts were asked, to the best of their knowledge, what are the most widely used and/or effective public and private enforcement measures in their country.

In the EU, starting with France, the expert mentioned the graduated response system run by HADOPI, but expressed doubts as to its effectiveness. He also pointed out as an effective private measure the legal provision in Article L.335-2-1 IPC that prohibits acts in relation to software that enables copyright infringement (see *Radioblog* and *eMule* cases). In Germany, the most widely used and most effective enforcement measure is the cease-and-desist letter. In the Netherlands, the issuing of court orders to require Internet access providers to block access to infringing websites is particularly popular, although there is debate (even at judicial level) on how to assess its efficiency. It is also common for Dutch intermediaries to employ voluntary NTD procedures, according to the aforementioned code of conduct in place for ISPs in the Netherlands. Finally, *Stichting BREIN* frequently initiates civil enforcement actions against large-scale infringers. In Poland, the most common measures are civil law injunctions and orders of damages based on the amount of double license fees. Sanctions against intermediaries are rare.

In Spain, there has been frequent use of injunctions by the CPI (sec. 2) to remove and block access to infringing content, disconnect the Internet service of infringers and cancel or block “.es” domain names or infringing websites (e.g. *RojaDirecta* cases). Criminal sanctions introduced in 2015 are only recently starting to be issued and drawing media attention. The expert also noted a 2015 administrative procedure, where all Spanish ISPs were ordered by the CPI (sec. 2) to suspend service and block access within 72 hours to any websites identified as belonging to *The Pirate Bay* group. Finally, it was noted that CMOs typically notify ISPs about infringing content available on their websites and threaten with judicial action unless that content is blocked or removed/delisted, a practice that appears to be effective.

In Sweden, the information injunction is a particularly effective measure for copyright holders to receive all the necessary details for further proceedings. A cease-and-desist letter typically follows this injunction. Right holders have also effectively initiated civil or criminal court proceedings against

individuals primarily to stop infringement, rather than to obtain damages. The expert also notes that public prosecutors take on cases involving mere sharing of content (rather than only high-profile, commercial and large scale infringements). Regarding injunctions against intermediaries, a Swedish court issued in 2017 the first ever injunction ordering an ISP to block its customers' access to a number of IP and http addresses relating to a website (*The Pirate Bay*). Despite that, it was noted that Swedish law requires at least a showing of contributory infringement (except for information injunctions) which, combined with the absence of more specific rules beyond safe harbors, arguably disincentivizes ISPs from developing common codes of conduct for NTD procedures.

Finally, in the UK, injunctions against service providers under Section 97A CDPA are widely used: more than 500 injunctions were granted according to 2015 numbers. Most of the case law in this respect has concerned blocking injunctions, such as against unauthorized sports live streaming websites and websites like *Popcorn Time*.

Outside Europe, in Brazil, the most effective measures are those carried out directly against intermediaries as private enforcement, such as the sending of out-of-court notifications and in general the judicially created NTD system. As described by the expert, in the current judicial interpretation of the law, an ISP can be held secondary liable if it does not make an URL to infringing material inaccessible after being notified by the interested party. In Canada, the most common measures are infringement notices sent by right holders via intermediaries through the notice-and-notice system or (less frequently) by way of a Norwich order. Canadian copyright holders have reportedly sent millions of notices since the law came into force in early 2015. Conversely, copyright holders have not launched many civil infringement and anti-circumvention proceedings against users and intermediaries. Finally, it is worth noting the current and controversial discussion in Canada on the possible implementation of a copyright web-blocking mechanism, to be managed by an independent third-party agency (the proposed Internet Piracy Review Agency), enforced by the the Canadian Radio-television and Telecommunications Commission, and operating under the Telecommunications Act. As of writing, no decision regarding its implementation has been made.

Turning to Asia, in Hong Kong, the most widely used private enforcement measures are takedown notices issued to local and foreign online intermediaries, and infringement notices issued to alleged infringers. From the perspective of public enforcement, the most common measure is reporting to (or cooperating with) the Customs and Excise Department, which inter alia monitors popular online forums to track and arrest users uploading infringing content.

In Indonesia, the filing of criminal complaints for copyright infringement is the most common measure. The expert also points to the administrative provisions that allow for the possibility of closing a website following reporting of an infringement to an ISP, as well as a new infringing website list that identifies the most popular piracy websites in Indonesia and encourages advertisers to remove their ads therefrom. Media reports indicate that at least 300 infringing websites were blocked as a result of this program.

In Japan, there is significant litigation involving information injunctions under the regime of the ISP Liability Limitation Act. In addition, the Intellectual Property Policy Headquarters recently published the emergency plan against copyright infringing websites (April 2018), encouraging ISPs to conduct a site-blocking under certain conditions and announcing the establishment of a legal system for enabling such site-blocking by ISPs.

Finally, in Thailand, the most widely used enforcement practice is public criminal enforcement by police authorities, which is considered to be the most convenient and cost effective measure. Also common are direct warnings for the removal of infringing content, a private enforcement practice prior taking place before the start of a criminal procedure. As for the different injunctions against intermediaries described above, they have only recently entered into force, making it difficult to assess their popularity or effectiveness.

CONCLUSION

To conclude, despite some legal uncertainty, most acts studied are qualified as direct copyright infringement by users or give rise to liability of intermediaries. Moreover, ISPs are often subject to injunctions and duties of care even when they benefit from safe harbours. On the whole, copyright holders have a vast arsenal of legal enforcement measures to deploy against end-users and ISPs. There is a trend in many of the countries studied towards copyright enforcement through civil or administrative measures aimed at blocking websites that provide access to infringing content. Notices to infringers or platforms hosting or linking to infringing content with the aim of removing/blocking such content are likewise regularly used, the latter in the context of NTD systems. Criminal measures are less popular.

Still, despite the abundance of enforcement measures, their perceived effectiveness is uncertain. Therefore, it is questionable whether the answer to successfully tackling online copyright infringement lies in additional rights or enforcement measures, especially if these will not lead to additional revenue for copyright holders and risk conflicting with fundamental rights of users and intermediaries. Instead, it might be sensible to search for the answer to piracy elsewhere, on the provision of affordable and convenient legal access to copyright-protected content.

1. Introduction and Methodology

The Institute for Information Law (**IViR**) of the University of Amsterdam and Ecorys conducted a research project on online copyright infringement.⁵ In this project, “online copyright infringement” means the online use of protected music, films and TV series, books, and video games covered by an exclusive right (under copyright and related rights) but not authorized by the right holders or otherwise permitted under the applicable law (e.g. by virtue of an exception or limitation).⁶

The research project focuses on the impact of online copyright infringement on online and offline sales and consumption. It distinguishes four main online and offline channels to acquire or consume the types of content mentioned: (1) Physical carriers (CD, DVD, blu-ray, print); (2) Legal digital: downloading and streaming, free and paid-for; (3) Live attendance to concerts and cinemas, as well as merchandise purchase; (4) Illegal channels, such as unauthorized streaming websites, P2P platforms, cyberlockers, newsgroups, and Kodi boxes. One of the aims of the study is to provide factual information about the state of online copyright infringement in different countries. The present legal report contributes to this part of the project.

This legal report is based on desk research and the analysis of questionnaires completed by legal experts in thirteen countries, including seven European Union (**EU**) member states (France, Germany, Netherlands, Poland, Spain, Sweden, and United Kingdom), two American countries (Brazil and Canada), and four Asian countries (Hong Kong, Indonesia, Japan, and Thailand). The questionnaires were subject to comments and review. **ANNEX 1** reproduces the questionnaire sent to each country and **ANNEX 2** contains a copy of the final version of all national responses to the questionnaires.⁷

The purpose of the questionnaire was to gather legal information for each country. The focus of the questions is on quantitative and qualitative information that describes the legal situation of online copyright infringement in each country, including copyright enforcement by public authorities and right holders. The questionnaire concerns the legal status of online copyright infringement and enforcement under “national law”, an umbrella term encompassing both statute law and case law. The questions are divided into two subsections. The first addresses substantive legal rules on online copyright infringement in national law. The second refers to national enforcement measures, procedures, remedies and sanctions.

This legal report provides a descriptive overview of how these issues are addressed under national law. It follows the structure of the questionnaire and proceeds as follows. After this introduction, **section 2** provides an overview of the international and regional legal framework that is relevant to provide context to the national answers.

Section 3 examines substantive legal rules on online copyright infringement in national law. This entails, first, an assessment of the online acts qualified as copyright infringement under national law (**3.1**). For this purpose, the report addresses a catalogue of specific activities (downloading, streaming, stream-ripping, uploading, hyperlinking, the sale of kodi boxes or similar devices), identifies other types of unauthorized use beyond this catalogue, and provides an overview of legal uncertainty areas. On the basis of this analysis, an assessment is made of the relevance of different elements for infringement, namely: knowledge, commerciality, and type of copyright-protected content (**3.2**). This

⁵ For the purposes of this report and the questionnaires the term “copyright” includes also related or neighboring rights.

⁶ Online copyright infringement is also sometimes referred to as online “piracy”, a term avoided in this legal report due to its lack of clarity.

⁷ Reports received from: France, Brad Spitz (hereafter: **Report France**); Germany, Franz Hofmann (hereafter: **Report Germany**); Netherlands, Stef van Gompel (hereafter: **Report Netherlands**); Poland, Tomasz Targosz (hereafter: **Report Poland**); Spain, Raquel Xalabarder (hereafter: **Report Spain**); Sweden, Kacper Szkalej (hereafter: **Report Sweden**); United Kingdom, Christina Angelopoulos (hereafter: **Report UK**); Brazil, Allan Rocha Souza & Luca Schirru (hereafter: **Report Brazil**); Canada, David Fewer (hereafter: **Report Canada**); Hong Kong, Alice Lee (hereafter: **Report Hong Kong**); Indonesia, Henry Soelistyo (hereafter: **Report Indonesia**); Japan, Tatsuhiro Ueno (hereafter: **Report Japan**); Thailand, Ning (Nontaya) Chulajata and Fabrice Mattei (hereafter: **Report Thailand**).

is followed by an examination of national rules on the liability of online intermediaries, namely available liability exemptions and areas of uncertainty (3.3). The section closes with a description of the treatment of copyright infringement by minors in different national laws (3.4).

Section 4 analyses enforcement measures, procedures, remedies and sanctions. It starts by examining the application of civil, administrative, and criminal measures against users (4.1) and online intermediaries (4.2). It then looks into differences between private and public enforcement per type of content (4.3), the issue of disclosure of personal data in the context of enforcement (4.4), the entitlement to apply for enforcement measures (4.5), and the most used and effective enforcement measures in national law (4.6).

2. Legal Background: International and EU Copyright Law

National copyright law does not exist in a vacuum. It is part of a multi-level system that comprises international treaties and conventions, as well as regional treaties and legislation. This international and regional legislation significantly harmonizes rules on substantive copyright law and enforcement. The countries in this study are party to all or some of the main international treaties on copyright, which shape their national laws. For that reason, section 2.1 briefly outlines the relevant treaties, their basic rules and minimum standards. In addition, EU member states are subject to a high level of harmonization stemming from a large number of directives on copyright and related rights, the interpretation of which is determined by the case law of the Court of Justice of the EU (CJEU). Section 2.2 provides an overview of these rules, as they are crucial to understand the national laws of EU member states.

2.1. International Law

For our purposes, the most relevant international treaties and conventions in copyright law are the Berne Convention for the Protection of Literary and Artistic Works (**BC** or **Berne**), the 1994 Agreement on Trade-Related Aspects of Intellectual Property Law (**TRIPS**) and, in relation to use over digital networks, the 1996 WIPO Copyright Treaty (**WCT**) and WIPO Performances and Phonograms Treaty (**WPPT**).

The membership status of all countries can be summarized as follows. First, EU member states are parties to all international agreements. The EU as an organization is a member of TRIPS and the WIPO Treaties, making them binding on its institutions and Member States.⁸ Second, all countries are party to the BC and to the latest amended version of TRIPS. Third, most countries are party to the WIPO Treaties, with the exception of Brazil and Thailand, which are not members of either.⁹

Berne Convention

The BC is the first major international treaty on copyright.¹⁰ Its main principles are national treatment, automatic protection (or prohibition of formalities), and independence of protection in the country of origin of the work.¹¹ Berne sets out minimum standards regarding the protection of works, the rights of authors, and term of protection. Protected works include “every production in the literary, scientific

⁸ Cf. Art. 216 TFEU the WIPO Treaties were approved on behalf of the European Community by Council Decision 2000/278/EC.

⁹ NB Hong Kong is party to these agreements by virtue of China’s accession thereto and specific declarations / notification that clarify this membership. Note also that Japan, Hong Kong, and Canada made specific declarations and reservations regarding certain provisions in the WPPT.

¹⁰ The BC was concluded in 1886. It was revised in Paris (1896) and at Berlin (1908), completed at Berne (1914), revised at Rome (1928), at Brussels (1948), at Stockholm (1967) and at Paris (1971), and was amended in 1979.

¹¹ See, respectively, Arts 5(1), 5(2) and 5(3) BC.

and artistic domain, whatever the mode or form of its expression”.¹² Authors are granted a series of exclusive rights, such as translation, reproduction, public performance, broadcasting, public recitation, and adaptation.¹³

The BC allows uncompensated exceptions or limitations to exclusive rights, including for certain types of reproductions, for quotations, reporting of current events, and ephemeral recordings for broadcasting.¹⁴ Article 9(2) BC applies to the reproduction right the first international version of the so-called three-step test: a set of three conditions that regulate the imposition and permissible scope of limitations to copyright.¹⁵ Finally, as a rule, the duration of copyright is set at 50 years after the death of the author.¹⁶

The TRIPS Agreement

The TRIPS Agreement is an annex to the agreement establishing the World Trade Organization (WTO). The main principles of the agreement are national treatment and most-favored-nation treatment.¹⁷ The agreement sets out minimum standards concerning the availability, scope and use of intellectual property rights, including provisions on copyright and related rights. The minimum standards concern protected subject matter, rights conferred, permissible exceptions or limitations to those rights, and the minimum terms of protection.¹⁸

Regarding *copyright*, TRIPS incorporates by reference the substantive provisions of the latest version of the BC, except those on moral rights.¹⁹ As a result, they become obligations under TRIPS as between its members. Beyond that, TRIPS includes obligations regarding subject matter and rights not covered by the BC, namely computer programs, databases, and rental rights for at least computer programs and (in certain circumstances) cinematographic works.²⁰ In this sense, TRIPS is a “Berne-plus” agreement. On limitations and exceptions, Article 13 includes the TRIPS version of the three-step test. Compared to the BC, this version replaces “authors” with “the right holder”, broadening the scope of the provision to derivative right holders.²¹ It also extends the test to new rights provided for in TRIPS.²²

For *related rights*, the agreement grants minimum rights for performers, producers of sound recordings and broadcasting organizations. The term of protection is of at least 50 years for the first two categories of right holders, and 20 years for the latter.²³

In addition to minimum standards, TRIPS includes rules on *enforcement* of intellectual property rights, namely general obligations on civil and administrative procedures and remedies, provisional measures, special requirements related to border measures, and criminal procedures (e.g. for willful

¹² Art. 2(1) BC.

¹³ See, respectively, Arts 8, 9, 11, 11bis, 11ter, and 12 BC. Minimum standards also include moral rights (Art. 6bis).

¹⁴ See, respectively, Arts 9(2), 10, 10bis, and 11bis(3) BC.

¹⁵ According to the test, and in general terms, copyright limitations must: (1) Be certain special cases, (2) Not conflict with the normal exploitation of the work, (3) Not unreasonably prejudice the legitimate interests of the author or rights holder.

¹⁶ See Art. 7 BC, which includes exceptions to this general rule, e.g. for anonymous or pseudonymous works, as well as works of applied art and photographic works.

¹⁷ Arts 1(3), and 3 to 5 TRIPS. In simple terms, these rules allow for the survival of BC exceptions to national treatment and, where material reciprocity is allowed, for a consequential exception to most-favored-nation treatment. See https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm.

¹⁸ Arts 9 to 14 TRIPS.

¹⁹ Art. 9(1) TRIPS, incorporating Arts 1–21 BC, except Art. 6bis.

²⁰ See, respectively, Arts 10.1, 10.2, and 11 TRIPS. NB members can extend the rental right to other subject matter. See Dreier and Hugenoltz, in: Concise Copyright (2016), ‘TRIPS’, Art. 11, note 1, p. 228.

²¹ NB TRIPS contains slightly different versions of the test in the fields of trademarks (Art. 17), designs and models (Art. 26(2)) and patents (Art. 30).

²² This includes rental of computer programs and cinematographic works. See Art. 11 TRIPS. Regarding copyright, the test was interpreted by a WTO Panel in: United States: Sec. 110(5) of the US Copyright Act, Report of the Panel, June 15, 2000, (00-2284), WT/DS160/R.

²³ Art. 14 TRIPS.

copyright infringement on a commercial scale). Furthermore, disputes between members concerning these obligations are subject to WTO dispute settlement procedures.²⁴ The enforcement procedures and the access to dispute settlement are significant for copyright, as they do not exist in the BC framework.²⁵

The WIPO Treaties

The 1996 WIPO Treaties comprise the WCT and WPPT. The aim of both treaties is to adapt copyright and related rights to the digital environment. The WCT is a special agreement within the meaning of Article 20 BC. Like TRIPS, it incorporates by reference the substantive provisions of the latest version of the BC, and adds to the BC *acquis* two additional categories of protected works: computer programs and databases.²⁶ In what concerns rights conferred, the WCT recognizes those granted in Berne but adds rights of distribution, rental, and a general right of communication to the public that applies to online use.²⁷ For the online environment, the rights of reproduction and communication or making available to the public are particularly important.

The WCT provides for an exclusive *reproduction right* with broad application in the digital realm. The right arguably includes all forms of incidental, transient or technical copies.²⁸ Article 9(1) BC already granted authors the exclusive right of authorizing the reproduction of works “in any matter or form”.²⁹ Article 1(4) WCT stipulates that the “Contracting Parties shall comply with Articles 1 to 21 and the Appendix of the Berne Convention”, and the corresponding Agreed Statement qualifies “the storage of a protected work in digital form in an electronic medium” as a reproduction within the meaning of Article 9 BC.³⁰

Regarding *communication to the public*, the BC had previously divided this concept into specific rights to perform, broadcast and recite.³¹ Article 8 WCT extends Berne’s subject matter and scope to the right of making works available to the public “in such a way that members of the public may access these works from a place and at a time individually chosen by them”. In doing so, it extends the application of copyright to interactive and on-demand acts of communication.³²

In the field of related rights, the WPPT builds on the 1961 Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (**RC** or **Rome**). The WPPT recognizes minimum standards of protection for performers and phonogram producers. Performers are granted, first, rights of broadcasting, communication to the public, and fixation regarding their unfixed (i.e. live) performances. Second, regarding their performances fixed in phonograms, performers are granted the rights of reproduction, distribution, rental, and making available.³³ Phonogram producers are granted rights of reproduction, distribution, rental, and making available regarding their phonograms.³⁴ Subject to reservations, performers and phonogram producers also have a right to remuneration for broadcasting and communication to the public of phonograms published for commercial purposes.³⁵

²⁴ See Part III TRIPS, Arts 41–64.

²⁵ NB Art. 33 BC on “disputes” grants jurisdiction on the interpretation and application of the Convention to the International Court of Justice. To date, no dispute has ever been brought to that court under this provision.

²⁶ See Arts 1, 4 and 5 WCT.

²⁷ Arts 6 to 8 WCT.

²⁸ Silke von Lewinski, ‘Certain Legal Problems Related to the Making Available of Literary and Artistic Works and Other Protected Subject Matter Through Digital Networks’ (2005) January–Ma UNESCO E-Copyright Bulletin 1, 5..

²⁹ In the context of related rights, the reproduction right is provided for in Arts 7, 10 and 13 RC.

³⁰ The Agreed Statements to Arts 7 and 11 WPPT contain similar provisions for performances and phonograms.

³¹ Paul Goldstein and P Bernt Hugenholtz, *International Copyright. Principles, Law, and Practice* (Third Edit, Oxford University Press 2013) 317–318..

³² *ibid* 318. Arts 10 and 14 WPPT respectively contain identical provisions for performers and phonogram producers.

³³ Arts 6 to 10 WPPT. Performers are also granted moral rights pursuant to Art. 5 WPPT.

³⁴ Arts 11 to 14 WPPT.

³⁵ Art. 16 WPPT.

Both WIPO Treaties contain additional similar provisions concerning exceptions or limitations, technological protection measures (TPMs), and rights management information (RMI). On *exceptions or limitations*, the treaties contain a version of the three-step test in Articles 10 WCT and 16 WPPT. The WCT test applies only to authors, like its Berne counterpart. Unlike the Berne version, the WCT test extends beyond the reproduction right, including limitations to all WCT-rights³⁶ and when applying Berne.³⁷ For its part, the WPPT test benefits performers and producers of phonograms. Both tests are accompanied by near identical Agreed Statements.³⁸

Both treaties impose obligations to provide adequate legal protection and effective legal remedies against: (1) the circumvention of effective TPMs used by authors, performers or phonogram producers in connection with the exercise of their rights and that restrict acts not authorized by right holders or permitted by law; and (2) the removal or alteration of RMI, as well as a number of unauthorized uses of works, phonograms or performances with knowledge that RMI on them has been removed or altered.³⁹

Finally, the WIPO Treaties contain “light” provisions on enforcement of rights mandating contracting parties to adopt measures to ensure application of the treaties. In concrete, they must ensure that enforcement procedures are available under their law so as to permit effective action against any act of infringement of rights covered by the treaties, “including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements”.⁴⁰ Nevertheless, no specific measures are prescribed.

2.2. EU law

The copyright *acquis communautaire* includes primary legislation, secondary legislation, and case law from the CJEU that form part of the EU legal order in the area of copyright. Primary law consists of the Treaties (TEU and TFEU) and the Charter of Fundamental Rights of the EU (**EU Charter**)—which has “the same legal value as the Treaties”⁴¹—together with fundamental or general principles of EU law developed by the Court, “including the requirement to protect fundamental rights”.⁴² The EU fundamental rights framework includes principles derived from the European Convention on Human Rights and national constitutional traditions, some of which are codified in the EU Charter.⁴³

³⁶ Art. 10(1) WCT applies to the newly granted rights in Arts 6, 7 and 8 WCT. See Andrew F Christie and Robin Wright, ‘A Comparative Analysis of the Three-Step Tests in International Treaties’ (2014) 45 IIC - International Review of Intellectual Property and Competition Law 409, 418–419., with a view that the wording in this paragraph allows countries to go beyond “certain special cases” based on a textual interpretation.

³⁷ Art. 10(2) WCT. This paragraph fulfils an “additional safeguard function” regarding exclusive rights in the BC. See Martin Senftleben, *Copyright, Limitations and the Three-Step Test. An Analysis of the Three Step Test in International and EC Copyright Law* (Kluwer Law International 2004) 121–124; P Bernt Hugenholtz and Ruth L Okediji, ‘Conceiving an International Instrument on Limitations and Exceptions to Copyright’ (2008) 20.

³⁸ The Agreed Statement on Article 10 WCT, adopted mutatis mutandis for Article 16 WPPT, states: “It is understood that the provisions of Article 10 permit Contracting Parties to carry forward and appropriately extend into the digital environment limitations and exceptions in their national laws which have been considered acceptable under the Berne Convention. Similarly, these provisions should be understood to permit Contracting Parties to devise new exceptions and limitations that are appropriate in the digital network environment. It is also understood that Article 10(2) neither reduces nor extends the scope of applicability of the limitations and exceptions permitted by the Berne Convention.”

³⁹ Arts 11–12 WCT and 18–19 WPPT.

⁴⁰ Arts 14 WCT and 23 WPPT.

⁴¹ Art. 6(1) first subpara. TEU.

⁴² Kieran St C Bradley, ‘Legislating in the European Union’ in Catherine Barnard and Steve Peers (eds), *European Union Law* (Oxford University Press 2014) 103..

⁴³ Griffiths, J., & McDonagh, L. (2013). Fundamental Rights and European IP Law: the Case of Art 17(2) of the EU Charter. In C. Geiger (Ed.), *Constructing European Intellectual Property. Achievements and New Perspectives* (pp. 75–117). Cheltenham: Edward Elgar.

Secondary law includes unilateral acts based directly on the Treaties, which must comply with primary law.⁴⁴ The most relevant acts for this report are the ten directives that have harmonized copyright and related rights in the EU.⁴⁵ These instruments have often surpassed international minimum standards of protection, on the pretext of *inter alia* removing disparities amounting to barriers to the free movement of goods and services.⁴⁶ The centerpiece of the copyright *acquis* is the 2001 InfoSoc Directive, which implements the WCT and WPPT into EU law and adapts it to the information society. Also relevant is the 2004 Enforcement Directive, which applies horizontally to all types of intellectual property rights. For this report, we must also take into account the 2000 E-Commerce Directive (**ECD**), which contains conditional liability exemptions or “safe harbors” for certain types of intermediary services.

EU law is an autonomous body of law largely independent from national law.⁴⁷ It is the exclusive jurisdiction of the CJEU, which has the power to provide authoritative interpretation on its rules, largely dependent on the obligation by national courts to refer cases under Article 267 TFEU.⁴⁸ Since 2009, there have been frequent references for a preliminary ruling on the interpretation of open concepts in the *acquis*, namely in the InfoSoc Directive.⁴⁹

The CJEU’s judgments play a vital role in shaping the law applicable to online use. This case law is largely influenced by a teleological method of interpretation, based on the application of the principles of effectiveness and autonomous interpretation, as well as a range of arguments linked to the objectives of EU copyright, found in the preambles of directives. A notable example is the interpretation of notions in directives as autonomous concepts of EU law, requiring uniform interpretation.⁵⁰ The InfoSoc Directive, in particular, is used as a horizontal harmonization instrument, with its recitals used as guidelines to this effect.⁵¹

It is also important to refer that the copyright directives are interpreted in respect of primary law *and* in light of the aforementioned international copyright agreements. This means that EU law must comply with international treaties⁵² and be interpreted in light of international law, “in particular where its provisions are intended specifically to give effect to an international agreement concluded by the Community”.⁵³

⁴⁴ *ibid* 103–104. Art. 288 TFEU contains a list of unilateral acts that are secondary sources of law, such as regulations, directives, decisions, opinions, and recommendations.

⁴⁵ The relevant directives are: the Software Directive (1991, amended and codified 2009); the SatCab Directive (1993); the Term Directive (1993, amended 2011); the Database Directive (1996); the Rental and Lending Rights Directive (1996, amended and codified 2006); the InfoSoc Directive (2001); the Resale Right Directive (2001); Enforcement Directive (2004); the Orphan Works Directive (2012); the CRM Directive (2014). Beyond the directives, the research considers other relevant “unilateral acts” in the field of copyright, such as decisions, opinions, recommendations, communications, white papers, and green papers. See Art. 288 TFEU.

⁴⁶ P Bernt Hugenholtz, ‘Copyright without Frontiers: The Problem of Territoriality in European Copyright Law’ in Estelle Derclaye (ed), *Research Handbook on the Future of Copyright* (Edward Elgar Publishing 2009) 17.

⁴⁷ Hannes Rösler, ‘Interpretation of EU Law’ 979, 979..

⁴⁸ Art. 19 TEU. See *ibid* 979–980.. Art. 267 TFEU gives the CJEU jurisdiction to give preliminary rulings concerning both the interpretation of primary law and the “the validity and interpretation of acts of the institutions, bodies, offices or agencies of the Union”.

⁴⁹ Due to doubts as to its competence basis and normative admissibility, some authors criticize this practice as “harmonization by stealth” or “judicial activism”. See Mireille Van Eechoud, ‘Along the Road to Uniformity – Diverse Readings of the Court of Justice Judgments on Copyright Work’ (2012) 3 *jipitec* 60; P Bernt Hugenholtz, ‘Copyright in Europe: Twenty Years Ago, Today and What the Future Holds’ (2013) 23 *Fordham Intellectual Property, Media & Entertainment Law Journal* 503, 513–521; Matthias Leistner, ‘Europe’s Copyright Law Decade: Recent Case Law of the European Court of Justice and Policy Perspectives’ (2014) 51 *Common Market Law Review* 559, 560–561; Marcella Favale, Martin Kretschmer and Paul LC Torremans, ‘Is There a EU Copyright Jurisprudence? An Empirical Analysis of the Workings of the European Court of Justice’ 31–32.

⁵⁰ See Christophe Geiger and Franciska Schönherr, ‘The Information Society Directive (Articles 5 and 6(4))’ in Irini Stamatoudi and Paul Torremans (eds), *EU Copyright Law. A Commentary* (Edward Elgar Publishing 2014) 554–556..

⁵¹ In general, see Rösler 979. For the copyright *acquis*, see Leistner 560, 599; Geiger and Schönherr 449–500.

⁵² See, in CJEU case law: *Laserdisken II*, para. 39; *Luksan*, para. 59; *DR and TV2 Danmark*, para. 29.

⁵³ See, in CJEU case law: *Peek & Cloppenburg*, paras 29–33; *Rafael Hoteles*, para. 35; *Murphy*, para. 189; *Infopaq I*, para. 32; *Painer*, para. 126; *UsedSoft*, para. 42; *Donner*, para. 23. An interpretation in light of international treaties can be understood as part of the Court’s systematic or contextual method of interpretation, as well as an express objective of the

InfoSoc Directive

The WIPO Treaties were implemented in the EU by the InfoSoc Directive, which harmonized several economic rights and adapted them to the digital age.⁵⁴ The harmonized rights are reproduction (Article 2), communication and making available to the public (Article 3), and distribution (Article 4).⁵⁵ The directive did not harmonize the right of adaptation, although different manifestations of the same can be found in the BC and national laws.⁵⁶

In EU law, and with the exception of distribution, these rights are susceptible of application to online use of works by individuals. The distribution right controls the “distribution of the work incorporated in a tangible article” and is subject to exhaustion under Article 4(2) InfoSoc Directive.⁵⁷ Hence, as a rule, this right does not apply online, despite specific derogations to this rule regarding computer programs and electronic lending of books.⁵⁸

Consistent with an international trend, Article 2 contains a broad *reproduction right* for authors and related rights owners: performers, phonogram producers, film producers, and broadcasting organizations.⁵⁹ Performers and broadcasters have a specific right of first fixation, meaning that the general reproduction right applies only to the reproductions of those fixations.⁶⁰

The scope of the right includes the prohibition of any direct or indirect, temporary or permanent reproduction by any means and in any form, in the whole or in part, of the works or subject matter of rights holders, with the exception of computer programs and databases.⁶¹ This broad scope results from the letter of the provision, the related recitals, and CJEU judgments that interpret the right in an expansive way and exceptions to it in a restrictive manner.⁶² As a consequence, the right increasingly applies to online dissemination of content, of which reproduction is an essential constituent, meaning that copies in technical sense become equivalent to legal reproductions⁶³, independently of their function or economic value.⁶⁴

Article 3 InfoSoc Directive grants authors a broad *right of communication to the public*, including *making available* (paragraph 1) and related right holders a narrower right of making available (paragraph 2). The distinction is justified because the directive leaves intact specific rights of communication recognized for the related rights holders elsewhere in the *acquis*.⁶⁵ The exclusive

InfoSoc Directive. See Favale, Kretschmer and Torremans 37, 52, 72.. The objective of consistency with international obligation is expressed in recitals 15 and 44 InfoSoc Directive.

⁵⁴ Recital 15 InfoSoc Directive.

⁵⁵ Arts 2, 3, and 4 InfoSoc Directive.

⁵⁶ P. Bernt Hugenholtz and Martin Senftleben, ‘Fair Use in Europe. In Search of Flexibilities’ (2011) 26–27.. Manifestations of the right of adaptation can be found in Arts 8, 12 and 14 BC.

⁵⁷ See recitals 28 and 29, Art. 3(3) InfoSoc Directive, barring exhaustion of the right of communication to the public of works and right of making available to the public other subject-matter.

⁵⁸ See João Pedro Quintais, *Copyright in the Age of Online Access: Alternative Compensation Systems in EU Law* (Kluwer Law International 2017) 159–171. (discussing the CJEU judgments in *UsedSoft* and *VOB*).

⁵⁹ Art. 2 InfoSoc Directive. See Ansgar Ohly, ‘Economic Rights’ in Estelle Derclaye (ed), *Research Handbook on the Future of EU Copyright* (Edward Elgar 2009) 217., noting that recitals 9 and 11 InfoSoc Directive seem to favor a “in dubio pro autore” interpretation of the right.

⁶⁰ Under Art. 7 Rental and Lending Rights Directive (“fixation right”).

⁶¹ See Art. 1(a) and (e) InfoSoc Directive. Arts 2–5 of this directive do not apply to software and databases, which are subject to special provisions in Arts 4–6 Software Directive and Arts 5–6 Database Directive.

⁶² See recital 21 InfoSoc Directive. For examples of CJEU interpretation, see.: *Infopaq I*; *Infopaq II*; *Murphy*; *SAS*.

⁶³ JP Triaille and others, *Study on the Application of Directive 2001/29/EC on Copyright and Related Rights in the Information Society* (2013) 120..

⁶⁴ Sari Depreeuw and Jean-Benoît Hubin, ‘Study on the Making Available Right and Its Relationship with the Reproduction Right in Cross-Border Digital Transmissions’ (2014) 41..

⁶⁵ See Art. 4 SatCab Directive and Art. 8 Rental and Lending Rights Directive, which remain applicable by virtue of Art. 1(2)(b) and (c) InfoSoc Directive. NB however that national laws may extend the exclusive right regarding linear rights of communication to the public online, “provided that such an extension does not undermine the protection of copyright”. See CJEU, *C More Entertainment*, paras 22–37, referring to broadcasts of sporting fixtures made live on the Internet under Art. 3(2)(d) InfoSoc Directive.

right applies to communication at a distance, covers online use, and is not subject to exhaustion.⁶⁶ The “making available” prong applies to interactive “on-demand” use (e.g. uploading), but does not require reception or access of the work by the public.⁶⁷

There is a vast CJEU case law on the right of communication to the public in the InfoSoc, SatCab and Rental and Lending Rights Directives.⁶⁸ These cases have shaped the interpretation of the right, including its applicability online. It is worth highlighting some of the main conclusions from these judgments, as they shape current domestic law of member states analyzed in this report and are cited frequently in responses to the questionnaire.

First, the right must be interpreted broadly.⁶⁹ Second, “communication to the public” is an autonomous concept of EU law.⁷⁰ As a result, the concept should have the same meaning and interpreted according to the same criteria whether it is used in the context of an exclusive right (in the InfoSoc Directive) or a remuneration right (in the Rental and Lending Rights Directive).⁷¹ Third, communication to the public involves different types of activities both offline and online.⁷² For the online world, relevant in the context of this report, the right has been applied to the “live streaming” or broadcasting by a third party over the Internet of signals from commercial television broadcasters (*ITV Broadcasting*), the provision of “clickable links” giving access to protected works (*Svensson*), the provision of framing links to protected works (*BestWater*), the direct broadcast of a sporting fixture on an Internet site (*C More Entertainment*), the posting of hyperlinks to works on third party websites without the right holder’s consent (*GS Media*), the sale of multi-media players with pre-installed add-ons that contain hyperlinks to websites making available works to the public without the consent of the right holders (*Filmspeler*), and the provision of an online peer-to-peer platform that enables the sharing of protected files without the consent of right holders (*Ziggo*).

To determine whether a use qualifies under Article 3 InfoSoc Directive, the court has developed a number of criteria and conditions. A use triggers the exclusive right if it meets two cumulative conditions: it is (1) an act of communication (2) to the public. An act of communication appears to require deliberate intervention by the user. That act is made “to the public” if it reaches an indeterminate and fairly large number of recipients as potential beneficiaries of the communication. In addition, the public in question must either be a “new public” (i.e. a public not taken into account by the copyright holder when they authorized the initial communication) or a public reached through a separate or specific technical means. In parallel to these cumulative conditions, the CJEU sometimes refers to the profit-making nature or purpose of the communication and other complementary and interdependent factors or sub-criteria, which are taken into consideration to varying degrees in order to make an individual assessment of the concept of communication to the public.⁷³

⁶⁶ Recital 25 InfoSoc Directive. See e.g. CJEU: *SCF*, para. 59; *C More Entertainment*, para. 26.

⁶⁷ Art. 3(3) and Recital 29 InfoSoc Directive. NB since the judgments in *Coditel I* and *II*, the CJEU has considered communication to the public to be a service and, therefore, not subject to exhaustion.

⁶⁸ These CJEU cases are, in chronological order: *EGEDA I*; *Rafael Hoteles*; *Airfield*; *Organismos Sillogikis*; *Murphy*; *Circul Globus*; *PPI*; *ITV Broadcasting*; *Svensson*; *OSA*; *BestWater* (Order); *Sociedade Portuguesa de Autores* (Order); *C More Entertainment*; *SBS*; *Reha Training*; *GS Media*.

⁶⁹ See recital 23 InfoSoc Directive. See: CJEU: *ITV Broadcasting*, para. 20 (and case-law cited therein); *OSA*, para. 23; *SBS*, para. 14; *Reha Training*, para. 36.

⁷⁰ CJEU, *Rafael Hoteles*, para. 31.

⁷¹ CJEU, *Reha Training*, paras 27–34.

⁷² On transmissions in hotels, see CJEU: *EGEDA I*; *Rafael Hoteles*; *Organismos Sillogikis*; *PPI*; *Sociedade Portuguesa de Autores*. On transmissions in a circus, see CJEU, *Circul Globus*. On transmissions in a spa establishment, see CJEU, *OSA*. On transmissions in the premises of a rehabilitation center, see CJEU, *Reha Training*. On transmissions in a public place (a pub), see CJEU, *Murphy*. On transmissions in a dental practice, see CJEU, *SCF*. Judgments involving different aspects of communication to the public by satellite include CJEU: *Lagardère*; *Airfield*; *SBS*.

⁷³ For a detailed analysis of this case law, see JP Quintais, “Untangling the hyperlinking web: In search of the online right of communication to the public”, *J World Intellect Prop.* 2018, pp. 1–36. <https://doi.org/10.1111/jwip.12107>.

Article 5 InfoSoc Directive contains the primary regulation for *exceptions or limitations* at EU level. It applies to all copyright subject matter, except software and databases.⁷⁴ Its first paragraph contains the directive's sole mandatory limitation, applying to transient or incidental copies.⁷⁵ Article 5(2) to (4) contains an exhaustive list of twenty optional limitations, applying to the otherwise exclusive rights of reproduction, communication to the public, and distribution.⁷⁶ Where member states choose to implement these, some are conditional upon the grant of fair compensation.⁷⁷ For the others, member states may nevertheless demand compensation in their national laws.⁷⁸ Article 5(5) contains the directive's version of the three-step test.

The regulation of TPMs and RMI is found in Articles 6 and 7 InfoSoc Directive. These provisions implement and go beyond the parent provision in the WCT (Articles 11 and 12) and WPPT (Articles 18 and 19). For our purposes, it is important to further explain the provision on TPMs. Article 6 instructs member states to provide adequate legal protection against the circumvention of effective TPMs, i.e. devices or components aimed at restricting unauthorized access to or use of works. "Access controls" are measures for protection of a work, such as encryption, scrambling or other transformation. "Use controls" refer to mechanisms that prevent, for example, the making of copies of works. The legal regime of TPMs includes protection against circumvention and preparatory acts.⁷⁹

Article 6(4) regulates the intersection between TPMs and exceptions or limitations, and mostly allows the first to override the second.⁸⁰ It contains a special rule on licensed interactive on demand services, which prohibits member states from implementing any measures limiting the effect of TPMs if the work in question is made available online for interactive on-demand transmission on agreed contractual terms.⁸¹ This includes right holders making available works online (under Article 3) for streaming or downloading on-demand. Thus, in such a "technology plus contract" scenario, all exceptions or limitations can be set aside.⁸²

Finally, Article 8 of the directive on *sanctions and remedies* implements the light obligations arising from the WIPO Treaties in this respect (Articles 14(2) WCT and 23(2) WPPT). The more detailed international provisions on enforcement laid out in TRIPS are implemented in the *acquis* by the Enforcement Directive.

Member States are required to adopt appropriate, effective, proportionate and dissuasive *sanctions* in respect of infringements of exclusive rights, TPMs or RMI (Article 8(1)). Additional obligations in this respect arise from the Enforcement Directive. Member States must also ensure that right holders

⁷⁴ Marie-Christine Janssens, 'The Issue of Exceptions: Reshaping The Keys to the Gates in the Territory F Literary, Musical and Artistic Creation' in Estelle Derclaye (ed), *Research Handbook on the Future of EU Copyright* (Edward Elgar 2009) 328..

⁷⁵ P Bernt Hugenholtz and others, 'The Recasting of Copyright & Related Rights for the Knowledge Economy (Executive Summary of Final Report)' (2006) 68–69.

⁷⁶ On the exhaustive nature of the list in Art. 5, see recital 32 InfoSoc Directive. The list contains four optional limitations for reproduction in Art. 5(2), fifteen optional limitations for reproduction and/or public communication in Art. 5(3), and the possibility to extend the previous limitations (applying to reproduction) to the right of distribution in Art. 5(4). NB Art. 5(3)(o) contains a deviation from the exhaustive nature of the list by including a "grandfathering clause" for pre-existing analogue uses of minor importance (*de minimis*).

⁷⁷ Namely, those in Art. 5(2)(a), (b) and (e) InfoSoc Directive.

⁷⁸ Recital 36 InfoSoc Directive.

⁷⁹ Art. 6(1)–(3) InfoSoc Directive. On the meaning of "effective" TPMs, see CJEU, *Nintendo*, paras 27–28.

⁸⁰ Janssens 334.

⁸¹ Art. 6(4), fourth subparagraph, and recital 53 InfoSoc Directive. "Agreed contractual terms" in this context seems to have a broad construction and likely applies also to standard form contracts such as typical online end-user licence agreements. See Silke von Lewinski and MM Walter, 'Information Society Directive' in MM Walter and S. von Lewinski (eds), *European Copyright Law. A Commentary* (2010) 1074, (n.482). For a more restrictive view, see Lucie Guibault and others, 'Study on the Implementation and Effect in Member States' Laws of Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (Final Report)' (2007) 112., arguing for the application of the provision solely to negotiated and agreed terms,

⁸² Art. 6(4), fourth subparagraph, and recital 53 InfoSoc Directive, excluding from the scope of the provision non-interactive Internet transmissions. See also Joost Poort and João Pedro Quintais, 'The Levy Runs Dry: A Legal and Economic Analysis of EU Private Copying Levies' (2013) 3 *jipitec* 205, 209.

whose rights are affected in their territory (by violation of Articles 2 to 4 and 6–7) to bring actions for damages and/or apply for injunctions and seizures (Article 8(2)). According to the CJEU, these provisions do not impose nor prevent member states from mandating Internet Service Providers (ISPs) to disclose personal data of their subscribers in the context of copyright infringement proceedings.⁸³

In addition, Article 8(3) obligates member states to ensure that rights holders can apply for injunctions against intermediaries whose services are used by a third party to infringe copyright. This possibility should be available even if the intermediary is not itself directly liable for infringement (and, thus, for damages under 8(1) and (2)).⁸⁴ Article 8(3) remains applicable despite the existence of a provision on injunctions in Article 11 Enforcement Directive.⁸⁵

Article 8(3) has played a significant role in the development of ISP liability, in articulation with the safe harbors in the ECD. In particular, although it is up to national law to determine the scope and procedures to seek injunctions, the same is limited inter alia by the operation of fundamental rights recognized in the EU Charter. This implies that an injunction must strike a fair balance between conflicting fundamental rights: to copyright as property, on the one hand (Article 17(2) EU Charter); and to the protection of personal data and privacy of Internet users, their freedom to receive information, and ISPs' freedom to conduct a business (Articles 7, 8, 11 and 16 EU Charter).⁸⁶

Enforcement Directive

The Enforcement Directive deals solely with *civil* (not criminal) *enforcement* of intellectual property rights, including copyright. It is without prejudice to international obligations in TRIPS (namely those relating to criminal procedures and penalties), national law provisions relating to criminal procedures or penalties for infringement, or other appropriate sanctions for infringement.⁸⁷

Other than general and final provisions, the directive includes chapters on enforcement measures procedures and remedies (II), sanctions by member states (III), and codes of conduct and administrative cooperation (IV).⁸⁸ Chapter II is most relevant for this report. It is divided into seven sections: general provisions; evidence; right of information; provisional and precautionary measures; measures resulting from a decision on the merits of the case; damages and legal costs; and publicity measures.

In general, enforcement measures, procedures and remedies shall be fair and equitable, not unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays. They should also be effective, proportionate and dissuasive, and be applied in such a manner as to avoid barriers to legitimate trade and to provide for safeguards against their abuse.⁸⁹

Certain measures in the directive are limited to infringements carried out on a “commercial scale”, including acts committed for “direct or indirect economic or commercial advantage” but excluding those “done by end consumers acting in good faith”. This includes measures related to certain types of evidence discovery (Article 6(2)), the right of information (Article 8) and precautionary seizure of movable or immovable property of the alleged infringer (Article 9(2)). Nonetheless, member states may also apply those measures in cases where infringement occurs on a non-commercial scale.⁹⁰

⁸³ CJEU, *Promusicae*. See also Bechtold, 2016, p. 485.

⁸⁴ See recital 59 InfoSoc Directive. See also CJEU, *LSG*.

⁸⁵ Recital 23 Enforcement Directive.

⁸⁶ The relevant CJEU case law in this respect includes *Scarlet Extended*, *Netlog*, *UPC Telekabel*, and *Bonnier Audio*.

⁸⁷ Arts 1, 2, and 16 Enforcement Directive.

⁸⁸ See Chapters II (Arts 3 to 15), III (Art. 16), and IV (Arts 17 to 19) Enforcement Directive.

⁸⁹ Art. 3 Enforcement Directive.

⁹⁰ Art. 2 and Recital 14 Enforcement Directive.

Regarding standing, the persons entitled to seek the measures are the right holders, authorized users (e.g. licensees), authorized CMOs, and professional defense bodies.⁹¹ The directive establishes a *presumption of authorship and ownership* of copyright in favor of authors and related right holders if their name appears on the work or other subject matter “in the usual manner”.⁹²

Although the Enforcement Directive generally covers interlocutory injunctions against intermediaries, the regulation of such injunctions for copyright infringement is dealt with by Article 8(3) InfoSoc Directive.⁹³ Upon a decision on the merits of the case, the directive mandates the application of corrective measures and *injunctions* for the prohibition of continuation of infringement against the right holder.⁹⁴ Non-compliance with an injunction may give rise to payment of a recurring penalty to the judicial authority and/or the injured party. These injunctions must also be available against intermediaries whose services are used by a third party to infringe copyright pursuant to Article 8(3) InfoSoc Directive.⁹⁵ Member states may provide for alternatives to these measures in the form of pecuniary compensation if such measures would cause disproportionate harm, the compensation “appears reasonably satisfactory”, and the infringer acted “unintentionally and without negligence”.⁹⁶

Right holders may also request for the payment of *damages* “appropriate to the actual prejudice suffered by him” against the infringer who “knowingly or with reasonable ground to know”, engaged in an infringing activity. Judicial authorities are competent to set the damages. In doing so, they have two options: (1) they may take into account “all appropriate aspects”, such as negative economic consequences (e.g. lost profits and unfair profits made by the infringer) and, if appropriate, non-economic factors (e.g. moral prejudice); or, alternatively, (2) set the damages as a lump sum on the basis of hypothetical royalties or fees for authorization of the infringing use.⁹⁷

If the infringer acted *without knowledge or reasonable grounds to know*, member states may allow judicial authorities to order the recovery of profits or payment of damages.⁹⁸ In addition, the directive states that the successful party in an infringement procedure may recover its “reasonable and proportionate” legal costs and other expenses (e.g. lawyer’s fees) from the unsuccessful party, unless this is prevented by equity.⁹⁹

Finally, the directive states that member states shall encourage the development of *codes of conduct* to assist the enforcement of intellectual property rights, and the submission to the Commission of drafts of such national or EU-wide codes, as well as evaluations thereof.¹⁰⁰

E-Commerce Directive (ECD)

In EU law, there’s no comprehensive harmonization of intermediary liability. The ECD contains conditional liability exemptions or “safe harbors” for certain types of intermediary services regarding claims for damages: mere conduit (or access), caching, and hosting (Articles 12 to 14). The directive further contains a general prohibition on the imposition of general monitoring obligations on intermediaries (Article 15).

⁹¹ Art. 4 Enforcement Directive.

⁹² Art. 5 Enforcement Directive. This provision therefore goes beyond the international standard set in Art. 15 BC, incorporated in TRIPS.

⁹³ Art. 9(1)(a) last sentence Enforcement Directive.

⁹⁴ See, respectively, Arts 10 (on corrective measures, referring e.g. to recall or definitive removal from the channels of commerce, as well as destruction of infringing goods) and 11 (on injunctions).

⁹⁵ Art. 11 and recital 23 Enforcement Directive.

⁹⁶ Art. 12 Enforcement Directive.

⁹⁷ Art. 13(1) Enforcement Directive.

⁹⁸ Art. 13(2) Enforcement Directive.

⁹⁹ Art. 14 and recital 26 Enforcement Directive.

¹⁰⁰ Art. 17 Enforcement Directive.

This regime does not prevent that intermediaries are required to take measures against the infringement of copyright. The measures may result from the possibility of injunctions against intermediaries available under the InfoSoc Directive, as well as from the imposition of duties of care allowed by the ECD.

In interpreting this constellation of provisions, the CJEU has noted that safe harbors require a sufficient degree of “neutrality” from the intermediary. There is therefore a grey area regarding the qualification of certain web 2.0 platforms as “neutral”/“passive” or as “active” intermediaries for the purposes of the hosting safe harbor in Article 14.¹⁰¹

The approach finds its legal basis in Recital 42 of the ECD, according to which the directive’s safe harbors are applicable only if the platform’s activities are of “a mere technical, automatic and passive nature”. For instance, in *Google France/Louis Vuitton*, this meant that a platform should play a “neutral” role with regard to the data it stores to enjoy safe harbor protection.¹⁰² When a platform plays “an active role of such a kind as to give it knowledge of, or control over, the data stored”, it falls outside the scope of the safe harbor.¹⁰³

The distinction between “active and “passive” role in this context is unclear. The CJEU has provided some guidance in this respect. Thus, in *L’Oréal/eBay* the Court stated that if the online sales platform eBay assists users in “optimising the presentation of the offers for sale in question or promoting those offers”, it does not merely play a neutral role but must be considered an active platform.¹⁰⁴ However, the mere fact that eBay “sets the terms of its service, is remunerated for that service and provides general information to its customers” does not mean it plays an active role.¹⁰⁵ By contrast, in *Google France/Louis Vuitton*, the role played by a platform in the drafting of a commercial message which accompanies an advertising link or in the establishment or selection of keywords was considered relevant in determining whether a platform is active or passive.¹⁰⁶

A further aspect of the legal framework is controversial. Article 15 ECD (supported by Recital 47) requires that a distinction be made between general monitoring obligations and obligations to monitor in specific cases. Whereas the earlier would be prohibited, the latter would be permitted. In *L’Oréal/eBay*, the CJEU found that “active monitoring of all the data of each of [a platform’s] customers in order to prevent any future infringement of intellectual property rights” is not allowed under Article 15 ECD.¹⁰⁷ In line with *L’Oréal/eBay*, the CJEU found in *Scarlet Extended* and *Netlog* that requiring a platform to actively monitor “almost all the data relating to all of its service users in order to prevent any future infringement of intellectual-property rights” is also prohibited under Article 15.¹⁰⁸ Thus, it remains unclear precisely what type of “specific” (as opposed to “general”) monitoring duties may be lawfully imposed on providers to prevent infringement, namely in what concerns pro-active measures like filtering.¹⁰⁹

¹⁰¹ In its case law, the CJEU has applied Art. 14 ECD to a search engine’s advertising service, an online sales platform, and a social networking platform. See CJEU, *Google France/Louis Vuitton*, *L’Oréal/eBay*, and *Netlog*.

¹⁰² CJEU, *Google France/Louis Vuitton*, para 114.

¹⁰³ Ibid., para 120.

¹⁰⁴ CJEU, *L’Oréal/eBay*, para 116.

¹⁰⁵ Ibid., para 115. See also CJEU, *Google France/Louis Vuitton*, para 116.

¹⁰⁶ CJEU *Google France/Louis Vuitton*, para 118.

¹⁰⁷ CJEU, *L’Oréal/eBay*, para 139.

¹⁰⁸ CJEU, *Netlog*, para 38. See also CJEU, *Scarlet Extended*, para. 40.

¹⁰⁹ The issue of what type of notice-and-action or pro-active measures can be adopted voluntarily or imposed on hosting platforms is further complicated in the EU by virtue of two recent developments: the endorsement of some of these measures in the context of the proposed Article 13 of the Draft DSM Directive (COM (2016)593 final); and the endorsement of voluntary measures of different types in the Commission Recommendation of 1.3.2018 “on measures to effectively tackle illegal content online”(C(2018) 1177 final). The analysis of these developments is outside the scope of this report.

3. Substantive rules on copyright infringement

This section examines the responses to questions on substantive legal rules on online copyright infringement in national law.¹¹⁰ This entails, first, an assessment of online acts qualified as copyright infringement under national law (3.1). On that basis, we analyze the relevance of different elements for infringement, namely: knowledge, commerciality, and type of copyright-protected content (3.2). This is followed by an examination of national rules on the liability of online intermediaries, namely available safe harbours and areas of uncertainty (3.3). Finally, the section closes with a description of the treatment of copyright infringement by minors in different national laws (3.4).

3.1. Online acts qualified as copyright infringement¹¹¹

The present sub-section discusses the legal status of different types of online use under national law. This determination is made with reference to a catalogue of online acts susceptible of infringing the exclusive rights of copyright owners, followed by a catch-all category meant to include other activities that may infringe copyright specific to a national law. The acts are identified below.

- Downloading copyright-protected content from illegal/unauthorized sources on the Internet.
- Streaming copyright-protected content from illegal/unauthorized sources on the Internet.
- Stream-ripping copyright-protected content, especially from illegal/unauthorized sources on the Internet.
- Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the right holder.
- Posting hyperlinks to copyright-protected content that has been made available online without the express authorization of the right holder.
- The sale of Kodi boxes or similar devices, especially with unauthorized add-ons linking to copyright-protected content made available online without authorization.

The catch-all category refers to “other types of unauthorized online use of copyright-protected content not listed above”.

For each act, we asked national experts to explain whether the legal qualification depends on the knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content, and the commercial or for-profit nature or intent of the use or user. We also asked whether the legal status of the use varies for the types of protected content relevant to our study (music, audio-visual, books, and video games) and, if so, how.

Finally, experts were asked to note whether the legal status of any act is uncertain and why. This uncertainty may result, for example, from the use not being clearly covered by exclusive rights, from it benefiting from an exception or limitation, from it being subject to implied consent, from lack of clarity regarding the illegal/unauthorized nature of the source, or from some other reason.

The following paragraphs describe the legal status for each type of act across these multiple dimensions.

Downloading

The question here is whether (and under what circumstances) downloading copyright-protected content from illegal/unauthorized sources on the Internet qualifies as copyright infringement. The example provided is downloading a file with a song from a P2P platform such as *The Pirate Bay*,

¹¹⁰ See Annex 1: Legal Questionnaire, Questions 1 to 6.

¹¹¹ This section deals with Question 3.

which is an *illegal/unauthorized* source. Differently, a *legal/authorized* source would be a service like iTunes in a country where that service has obtained the necessary authorizations from right holders. Both examples are on opposite sides of the spectrum of illegal/unauthorized vs legal/authorized sources of reproduction. This was intended to avoid bias in responses and allow respondents to address potential grey areas as to the status of the source of reproduction under national law.

Downloading involves making a permanent reproduction of a work. As such, the act is typically restricted under the exclusive right of reproduction. If the download is made from a legal/authorized source it is not infringing. However, it may be infringing when it is made from an illegal/unauthorized source, because it lacks the authorization of the right holder and is not privileged by an exception or limitation to the right of reproduction.

- EU

National laws of European countries in the study are heavily influenced by EU copyright law regarding the legal status of downloads. A download is an act of reproduction under Article 2 InfoSoc Directive, potentially privileged by the optional private copying exception in Article 5(2)(b). As noted, the exception does not apply to computer programs and databases, meaning that it cannot apply to video games if the national law protects this type of content as a computer program.

The case law of the CJEU on the right of reproduction and the private copying exception has clarified that downloading from *illegal/unauthorized* sources is outside the scope of the exception and, as such, constitutes copyright infringement.¹¹² Therefore, at least since *ACI Adam* (April 2014), the scope of the exception should be interpreted as excluding reproductions for private use to be made from an unauthorized source.

This appears to be the case for most EU member states. The Netherlands is a good example. Although the law was not amended following this decision, the CJEU decision was considered binding and as having immediate effect.¹¹³ Nevertheless, as noted below, at least in Poland the failure to amend the law after *ACI Adam* has led to uncertainty regarding the legal status of downloads.

Against this background, it can be said that the national laws of member states generally consider downloading from an *illegal/unauthorized* source to be copyright infringement, with minor differences.

In the first place, national laws consider downloading to be covered by the *right of reproduction*. In these countries, there is a *strict liability regime* (at least for the right of reproduction). That means, for *civil* liability purposes, that the application of copyright to downloading does not appear to depend on: (1) the knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content; or (2) the for-profit nature or intent of the use or user. In addition, there are no specific rules per type of protected content.

In the second place, all national laws have implemented the optional private copying limitation, with the exception of the UK. Therefore, under UK law, it can be concluded that downloading from unauthorized sources infringes copyright without the need to assess the application of an exception.¹¹⁴

For the remaining countries, we must establish whether the exception applies. As noted, the exception does not cover computer programs. In some member states, video games are protected as computer programs, namely in the Netherlands¹¹⁵, Poland¹¹⁶ and arguably in Sweden.¹¹⁷ For those countries, downloading of video games does not benefit from the exception.

¹¹² CJEU, *ACI Adam* and progeny.

¹¹³ Report Netherlands, citing Kamerstukken II 2013/14, 29 838, nr. 72, p. 3.

¹¹⁴ Report UK, citing leading cases *Twentieth Century Fox Film Corporation v Newzbin* [2010] EWHC 608 and *Dramatico Entertainment v British Sky Broadcasting* ([2012] EWHC 268) (*Dramatico v Sky* (No.2)).

¹¹⁵ Report Netherlands, Art. 45n of the Dutch Copyright Act.

In addition to computer programs and databases, some national laws exclude other types of content from the scope of the exception. That is for instance the case of Sweden regarding copies of entire books.¹¹⁸

Beyond these variations on subject matter scope, most national laws (in statute or judicial application) have similar conditions to determine the scope of the exception. This is due to the high level of harmonization resulting from the large body of CJEU judgments on private copying. As a result, where the exception is implemented, its scope does not include the making of permanent copies from unauthorized sources. Hence, these copies will infringe copyright.

While that is generally true, some nuances should be noted. In Germany, downloading only infringes copyright if the source is “obviously illegal”.¹¹⁹ In France, the act in question can be infringing also because it may not be a “private” use, as there are at least two people involved in the process (the downloader and the uploader).¹²⁰ In Spain, when a copy is made in the context of an online service with agreed contractual terms (e.g. iTunes), the exception applies only if those terms do not explicitly prohibit nor authorize the making of private copies. Outside this scenario, the download is either prohibited (i.e. infringing) or a contractually authorized copy (and thus not a private copy).¹²¹

Finally, there is legal uncertainty as to the application of the exception in Poland after *ACI Adam*. Prior to the judgment, the consensus was that the application of the exception did not depend on the legality of the source. Since the law was not amended following the judgment, commentators are divided on whether the situation remains the same until the law changes or current law must be interpreted in conformity with EU law.¹²²

- AMERICAS (BRAZIL AND CANADA)

In the American countries, the situation is different. In Brazil, there is some uncertainty regarding the extent to which private copies are restricted by exclusive rights and, if so, which copies would be privileged by the private use exception.¹²³

Under Canadian law, downloading from illegal/unauthorized sources is a restricted act of reproduction.¹²⁴ Furthermore, like in EU member states, Canadian copyright law is a strict liability regime. The application of copyright to acts of downloading does not depend on elements of knowledge or the commercial character or intent of use. Commercial infringers, however, face more stringent civil liability and criminal penalties, as noted below at 4.1.¹²⁵

The Canadian Copyright Act provides for two private copying exceptions. First, a general uncompensated exception that applies to most subject matter but requires that the copy does not come from an *illegal/unauthorized* source (Section 29.22). Second, a compensated exception (similar to EU law levy systems) for musical sound recordings (Sections 79 et seq.), which does not mention the legal status of the source of reproduction. This means that, at least for musical sound recordings, it is arguable that the act of downloading by users is not copyright infringement.

¹¹⁶ See Report Poland (Question 9).

¹¹⁷ See Report Sweden (Questions 3 a) and c), and 7-c)),

¹¹⁸ Report Sweden, Sec. 12 Swedish Copyright Act.

¹¹⁹ Report Germany, Sec. 53 German Copyright Act.

¹²⁰ Report France.

¹²¹ Report Spain, citing Art. 31.3 TRLPI.

¹²² Report Poland, see Art. 23 Polish Copyright Act.

¹²³ However, the Brazilian legislator was careful to expressly exclude any criminal liability for individual private copying activities (see Report Brazil).

¹²⁴ Report Canada, Art. 3(1) of the Canadian Copyright Act.

¹²⁵ Report Canada, citing *Bishop v. Stevens*, [1990] 2 S.C.R. 467, at 480; and *Compo Co. v. Blue Crest Music Inc.*, [1980] 1 S.C.R., at 375.

In addition, there appear to be no differences in the legal treatment per type of protected content.

- ASIA (HONG KONG, INDONESIA, JAPAN, THAILAND)

In **Hong Kong**, downloading from illegal/unauthorized sources is a restricted act of reproduction and thus infringes copyright. As with other national laws (EU member states, Canada), for purposes of civil liability, Hong Kong law is a strict liability regime. That is to say, knowledge of the source is irrelevant. However, the downloader may invoke a defense to infringement, if s/he can establish fair dealing for the purpose of research, private study, criticism, review, news reporting or education, and satisfy the specific acknowledgment and content removal requirements therein.¹²⁶ The application of this defense will be assessed on a case-by-case basis.

Downloading from illegal/unauthorized sources may also attract criminal liability, which however depends on the downloader's knowledge and on the purpose/context being in the course of trade or business.¹²⁷ Neither civil nor criminal liability depends on the type of downloaded content.

Japanese copyright law is unique in that it only qualifies as infringing downloading of digital sound or visual recording from illegal or unauthorized sources, even if for private use. In addition, liability appears to require that the downloader has knowledge of the recording being made available without authorization of the right holder. *A contrario*, downloading other types of content (e.g. e-books) does not infringe copyright, even if the source of the reproduction is illegal or unauthorized.¹²⁸

The law of **Thailand** bears some resemblance to EU law. Downloading qualifies under the right of reproduction and is potentially subject to a "personal use" exception. However, copies made from an illegal/unauthorized source are outside the scope of the exception, as they fail to meet its requirements (apparently deriving from the three-step test) that the personal use does not conflict with the copyright owner's normal exploitation and unreasonably prejudices his "legitimate right". Finally, there appear to be no differences in the application of the right or exception depending on the type of content (being clear that videogames are protected as computer programs). As a result, downloading from illegal or unauthorized sources infringes copyright.¹²⁹

Indonesian law sets the copyright infringement norms broadly, applying to all kinds of reproduction in any manner and in any forms, both permanently and temporarily.¹³⁰ In sum, downloading copyright-protected content from illegal/unauthorized sources on the Internet is illegal unless it is made for non-commercial purposes, in which case it will be considered to be for "personal interest" and covered by the exception or "fair dealings defense" in Article 46 of the Indonesian Copyright Act. There appears to be no specific requirement of source for the application of the exception.¹³¹

For a Summary Table of the analysis in this subsection, please refer to ANNEX 3: Summary Tables Question 3 – online acts qualified as copyright infringement.

Streaming

Passive streaming – meaning the reception or accessing of a stream – is a curious case. Its experiential nature and the fact that it translates into the making of temporary and/or transient partial copies of works typically in the random access memory (RAM) of devices raises doubts as to whether: (1) the

¹²⁶ Report Hong Kong, citing Secs 38-39, 41 and 41A of the HK Ordinance.

¹²⁷ Report Hong Kong, citing Secs 118(1)(f) or 118(2A) of the HK Ordinance.

¹²⁸ Report Japan, citing Art. 30(1)(iii) of the Japanese Copyright Act.

¹²⁹ Report Thailand, citing Secs 4, 15 and 27 Thailand Copyright Act.

¹³⁰ Report Indonesia, citing Art. 1(12) Indonesian Copyright Law 2014.

¹³¹ See Report Indonesia.

copy qualifies as a reproduction; and (2) if so, whether it is privileged by national exceptions for such copies.

In the **EU**, member states laws qualify these copies within the reproduction right, with two exceptions, influenced by the CJEU judgment in *Filmspeler*. Under Dutch law, it is only clear that passive streaming is a copyright relevant reproduction when it originates from a kodi box or similar device with pre-installed add-ons that link to content available online without the permission of the right holders. French law, for its part, is interpreted as not covering passive streaming unless the same is carried out via such a kodi box.¹³² Here, as in other instances, CJEU case law appears to extend the reach of the exclusive right and introduce some uncertainty as to its precise borders.

On the flipside, the Court's interpretation of the temporary/transient copy exception in Article 5(1) InfoSoc Directive led most national reporters to conclude that the national implementations of the same do not privilege passive streaming. That judgment, it is reminded, interprets the lawful use requirement of the exception as meaning something similar to lawful/authorized source. In other words, where and to the extent the right of reproduction applies to streaming, no exception shields the user, leading to a finding of infringement almost uniformly across all EU countries.¹³³

The situation is remarkably different in the **American** countries. Importantly, neither in Brazil nor in Canada the courts have had a chance to weigh in on this topic. Although the legal status of streaming is uncertain in Brazil, it is more likely than not that it is non-infringing.¹³⁴ As for Canada, the reporter presents two options. First and most likely, copyright does not extend to passive streaming due to its *experiential* character. Alternatively, the use may qualify as a temporary reproduction. If it does, users are shielded from liability by the exception for technically essential temporary or transitory copies.¹³⁵

In **Asia** the situation varies, but it's mostly uncertain, due to the absence of case law. In **Thailand** passive streaming from unauthorized sources likely qualifies as a reproduction that is not privileged by the exception for "unavoidable temporary copying".¹³⁶ Conversely, under **Hong Kong** law it seems like receiving streams is outside the scope of copyright, whereas **Japanese** law leads to an outcome similar to Canadian law: the act is probably outside copyright, but if it qualifies as a transient reproduction in part, then is probably privileged by an exception for copies "required for the exploitation of works on computers".¹³⁷ Also in Indonesia the act of streaming appears to be covered by the exclusive right and not privileged by any limitation.¹³⁸

For a Summary Table of the analysis in this subsection, please refer to ANNEX 3: Summary Tables Question 3 – online acts qualified as copyright infringement.

Stream-ripping

For the most part, stream-ripping from illegal/unauthorized sources gets the same legal treatment as downloading in every national law. This makes sense, as in both instances the user makes a permanent copy of the work from an unauthorized source. However, some nuances merit pointing out.

¹³² See Reports France and Netherlands.

¹³³ But see the specific case of Poland, where this outcome is uncertain due to the potential application of the private copying exception here. On the latter, see *Downloading* supra.

¹³⁴ Report Brazil.

¹³⁵ Sec. 30.71 Canadian Copyright Act.

¹³⁶ Sec. 32.2 of the Thailand Copyright Act.

¹³⁷ Report Hong Kong; Sec. 47octies of the Japanese Copyright Act.

¹³⁸ Report Indonesia, although on this particular topic it is unclear whether the national expert is referring to active or passive streaming.

First, the novelty of the technique leads to legal uncertainty on the application of the exclusive right, both as a matter of the law in the books and the law in practice (i.e. near total absence of case law in this respect).¹³⁹

Second, there is a high degree of uncertainty as to whether ripping a stream can qualify as the circumvention of a (copy control) TPM, in which case the qualification as infringement may require in addition a subjective element of knowledge, awareness or intent.¹⁴⁰ For this to be the case, it appears that *a stream must itself be qualified as a TPM*, which is doubtful.

Third, it should be noted that in many instances stream-ripping occurs from platforms authorized by copyright holders or shielded by safe harbors, such as Netflix or YouTube. In these cases, the source itself is not illegal but rather an authorized online service provider. To be sure, the ripping may be a violation of the service provider's terms of service, a consideration that may or may not affect the legal status of the act in the eyes of the law. In the EU, for example, following the CJEU's restrictive case law on the private copying exception, this fact pattern may cause the ripped copy to fail the lawful/authorized source requirement (see *supra* on *downloading*). However, in the absence of clear guidance from statute or case law in this respect, the legal status of this activity remains uncertain.

For a Summary Table of the analysis in this subsection, please refer to ANNEX 3: Summary Tables Question 3 – online acts qualified as copyright infringement.

Uploading

Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the right holder is almost universally qualified as copyright infringement.

In the **EU**, it either infringes the right of reproduction and communication to the public (France, Poland, Sweden, and arguably UK), or solely the latter right, namely its making available prong (Germany, Netherlands, Spain). No exception applies.

In **Brazil**, the situation is similar, although the infringed rights are those of communication the public and (probably) distribution.¹⁴¹ Under **Canadian law**, although uploading qualifies as a restricted act of making available, there is a possibility that two distinct provisions may allow a work to be uploaded to a website or online platform (often not in full): the exception for non-commercial user-generated content; and the limited fair dealing user *rights* for purposes of research, education, parody or satire.¹⁴²

Finally, all **Asian countries** consider uploading of this type to be a restricted communication to the public.¹⁴³ Only Hong Kong allows for the possibility that the act may in certain cases be exempted by the application of a fair dealing *defense*.¹⁴⁴

For a Summary Table of the analysis in this subsection, please refer to ANNEX 3: Summary Tables Question 3 – online acts qualified as copyright infringement.

¹³⁹ E.g. Reports Netherlands, Brazil and Canada.

¹⁴⁰ E.g. Reports France, Germany, UK, Japan, and Thailand.

¹⁴¹ Arts 104 and 105 of the Brazilian Copyright Act.

¹⁴² Secs 29 and 29.21 of the Canadian Copyright Act. See Report Canada, constrating the broad interpretation of fair dealing purposes by the Supreme Court (CCH Canadian Ltd. v. Law Society of Upper Canada, 2004 SCC 13 (CanLII), at para. 51) with the stricter approach by the Federal Court in a 2017 parody case (*United Airlines, Inc v Cooperstock*, 2017 FC 616 (CanLII), < <http://canlii.ca/t/h4jzk> > at para 123).

¹⁴³ Reports Hong Kong, Indonesia, Japan and Thailand.

¹⁴⁴ Report Hong Kong.

Hyperlinking

In this question we asked national experts whether the posting of hyperlinks to copyright-protected content that has been made available online without the express authorization of the right holder amounts to copyright infringement. We additionally asked them to specify whether the answer varies depending on the type of hyperlinking technique in question, for example if the link at stake is a standard surface hyperlink, a deep-link, an embedded or framing hyperlink. As an initial remark, it appears that the hyperlinking technique used does not influence the legal qualification of the act in any of the national laws under examination.

The legal status of hyperlinking is a matter of great legal controversy in **Europe**. As noted, the CJEU has developed a complex line of case law including judgments on different types of online use, including hyperlinking (*supra* at 2.2). Since *GS Media*, the Court has made the qualification of hyperlinking to content available online without authorization of the right holder subject to a knowledge test tied to a for-profit condition. If the linker “knew or ought to have known that the hyperlink he posted provides access to a work illegally placed on the internet” (e.g. if “he was notified thereof by the copyright holders”), the provision of the link is a restricted communication to the public. To determine knowledge, a distinction is drawn between whether a person posting the link pursues profit or not. If s/he does, there is a rebuttable presumption that the linker had full knowledge of the legal status of the work, as s/he would “carry out the necessary checks” for that purpose. If the presumption is not rebutted, the link is assumed to communicate the work to a new public.¹⁴⁵ Although less detailed in their analysis, the subsequent judgments in *Filmspeler* and *Ziggo* have gone in the same direction.¹⁴⁶

As a whole, despite the legal uncertainty surrounding the application of the knowledge test and for-profit condition, all national reporters conclude on the basis of this CJEU case law that the hyperlinks at issue qualify as copyright infringement, as they fall under the right of communication to the public (making available) and are not privileged by an exception. This is remarkable insofar as it represents a departure from the understanding of copyright as a strict liability regime, where the deliberate or negligent qualification of the user’s intervention is relevant only to assess remedies.¹⁴⁷ For these hyperlinks, a finding of infringement will depend on whether the linker had the required knowledge of the unauthorized nature of the publication of the linked-to work. The obvious parallels with this construction are found in the realm of EU intermediary liability law (most notably in Article 14 ECD) and general unfair competition law.¹⁴⁸

One important deviation should be noted regarding Germany. This refers to a recent decision from the German Federal Court on a case concerning links in the context of search engines, more specifically thumbnails of pictures available on the internet without the consent of the copyright holder. The Court ruled that the defendant did not infringe copyright, noting that in case of search engines there is no presumption that the user has knowledge whether the respective content has been published with the consent of the copyright holder or not.¹⁴⁹

Again, the situation differs in American and Asian countries. In **Brazil**, where the courts have yet to address the issue, it is unlikely that hyperlinking gives rise to primary liability. Rather, this act should

¹⁴⁵ CJEU, *GS Media*, paras 47–52.

¹⁴⁶ Quintais 2018 (forthcoming).

¹⁴⁷ Tomasz Targosz, ‘A New Chapter in the Linking Saga’ (*Kluwer Copyright Blog*, 2016) <<http://kluwercopyrightblog.com/2016/09/09/a-new-chapter-in-the-linking-saga-its-becoming-a-horror/>>; Martin Senftleben, ‘Copyright Reform, GS Media and Innovation Climate in the EU – Euphonious Chord or Dissonant Cacophony?’ [2016] *Tijdschrift voor auteurs-, media- en informatierecht* 130, 132.

¹⁴⁸ *ibid* 132. Generally on EU intermediary liability law, see Christina Angelopoulos, *European Intermediary Liability in Copyright: A Tort-Based Analysis* (Kluwer Law International 2017).

¹⁴⁹ Report Germany, citing German Federal Court: BGH, Urt. V. 21.9.2018 – I ZR 11/16.

fall within the realm of joint liability (solidarity) for infringement of the statutory provision on “distribution and other use”, provided the link points to an unauthorized source and is made in a commercial context.¹⁵⁰ In **Canada**, the courts have only addressed hyperlinking in a defamation case (*Crookes v. Newton*); in light thereof and the language of the statute, it is unlikely that the act gives rise to primary liability for copyright infringement.¹⁵¹

In **Asia**, despite the absence of case law, Hong Kong and Thailand domestic law apparently allow for the conclusion that hyperlinking is covered by the right of communication to the public as such, without the need to assess subjective elements. Given the lack of applicable exceptions, this would lead to a finding of infringement.¹⁵² Differently, **Japanese** law and case law do not support a finding of primary liability because the linked-to works are not being transmitted; rather, only the Internet address (URL) is. However, these types of hyperlinks can constitute a tort of secondary liability under the Japanese Civil Code, in particular a tort of facilitating the illegal public transmission of works.¹⁵³ Finally, under the law of **Indonesia**, posting hyperlinks is not considered copyright infringement as such links only mention the URL address pointing the relevant copyright content. Consequently, there is no actionable reproduction or making available of the relevant works to the public. It should be noted however the lack of case law on this topic.¹⁵⁴

For a Summary Table of the analysis in this subsection, please refer to ANNEX 3: Summary Tables Question 3 – online acts qualified as copyright infringement.

Sale of Kodi boxes or similar devices

In **Europe**, the possibility that the sale of kodi boxes including by default add-ons that link to works available online constitutes direct infringement of the right of communication to the public was raised in *Filmpeleer*. The case involved the provision of a multimedia player sold online with pre-installed software that integrated third-party add-ons, which linked to different websites, including some containing works made available without the consent of right holders. Together with a user-friendly interface and a remote control, the device allowed users to easily access such works and stream them for viewing on a television screen. Importantly, advertising for the device singled out its ability to allow viewing of unauthorized content. The question before the CJEU was whether the right of communication to the public covers the *sale* of kodi boxes of this type.¹⁵⁵

After establishing that the sale of kodi boxes amounts to an act of communication and is directed at the public, the Court turned to the *GS Media* precedent for guidance. In doing so, it noted the importance of prior consent of the right holder for every act of communication and restated the prior judgment’s knowledge test for assessing the legality of a link to unauthorized content.¹⁵⁶ Here, the kodi box was sold “in full knowledge of the fact that the add-ons containing hyperlinks pre-installed on that player gave access to works published illegally on the internet”, as attested by the advertisement to that effect. Furthermore, the device was sold for profit at a price that accounted for its ability to allow streaming of audio-visual works without the consent of the right holders. In this light, the knowledge presumption of *GS Media* was found to apply and the sale of such devices to constitute a communication to a new public.¹⁵⁷

¹⁵⁰ Art. 104 Brazilian Copyright Act.

¹⁵¹ Report Canada, citing *Crookes v. Newton*, 2011 SCC 47, [2011] 3 SCR 269. For a short description of the case and access to further sources, see Stanford CIS, World Intermediary Liability Map, *Canada*, <https://wilmap.law.stanford.edu/entries/supreme-court-canada-crookes-v-newton-2011-scc-47>.

¹⁵² Reports Hong Kong and Thailand.

¹⁵³ Report Japan citing: *Rocket News 24 Case* (20 June 2013); *Retweet Cases* (15 September 2016, 25 April 2018).

¹⁵⁴ Report Indonesia.

¹⁵⁵ CJEU, *Filmpeleer*, paras 15–23.

¹⁵⁶ *Ibid*, paras 47–49.

¹⁵⁷ *Ibid*, paras 50–53.

Before this judgment, most national laws would probably deal with this type of act under the heading of secondary or intermediary liability. For instance, under Polish law this could configure a tort of assisting in copyright infringements¹⁵⁸, whereas in Germany it could lead to contributory liability dependent on the seller's knowledge, or even be subject to "interferer liability" (*Störerhaftung*).¹⁵⁹ However, after the CJEU judgment, most national reporters consider that their national laws will be interpreted consistently with *Filmspeler*, meaning that the domestic rights of communication to the public should apply to the sale of kodi boxes with unauthorized add-ons.

Like with hyperlinking after *GS Media*, the assessment of primary liability relies on a knowledge test and the for-profit condition, shifting the analysis of the act away from the paradigm of strict liability. Since no exception applies, the sale of these devices will be infringing. Finally, it should be mentioned that French law contains in addition a specific rule prohibiting the provision (or encouragement of the use) of software to communicate unauthorized works to the public, which would apply to these scenarios.¹⁶⁰

The situation is far less certain in the **American countries**. In **Brazil**, the absence of any case law leads the reporter to conclude that such sale would probably qualify as copyright infringement. The main reason is that Brazil contains broadly worded economic exclusive rights applying to "any kind of use" of works, followed by a non-exhaustive catalogue of typical rights: reproduction, distribution, making available, etc.¹⁶¹ Such a broad scope could theoretically reach the sellers of kodi boxes with unauthorized add-ons, although this is not certain. **Canadian law** is currently in flux. The expert reports the grant of interlocutory injunctions in two cases: against the sale of set-top boxes and against a website providing add-ons for Kodi boxes.¹⁶² However, the legality of this activity is yet to be assessed in the context of a forthcoming judgment in the first of these cases.¹⁶³

Finally, regarding **Asian countries**, only **Thailand** considers this activity to be covered by the right of communication to the public, subject to conditions: the sales must be for profit and the sellers must know or should have known of the illegal provenance of the work thus accessed.¹⁶⁴ Here, again, we observe a shift away from strict liability. In opposition, despite the uncertainty due to lack of court decisions, the laws of Japan and Hong Kong would probably deal with these activities in the realm of secondary liability. In **Japan**, on the basis of an analogous Supreme Court case on the distribution of a memory card that modifies a software game, it is likely that the sale of kodi boxes constitutes a tort giving rise to secondary liability under the Japanese Civil Code.¹⁶⁵ In **Hong Kong**, sellers of such devices may attract civil liability under different heads: infringement by authorization; contributory infringement by common design; or promoting, facilitating or enabling circumvention of TPMs.¹⁶⁶ In **Indonesia**, copyright law does not specify the sale of Kodi boxes or similar devices as copyright infringement. The ITE Law (on "Information and Electronic Transactions") regulates the prohibition

¹⁵⁸ Art. 422 Polish Civil Code.

¹⁵⁹ In Germany, the concept of "interferer liability" (*Störerhaftung*) has been shaped by case law on the basis of Sec. 1004 German Civil Code (Claim for injunction). It applies to any person who has willfully made a causal contribution to the direct copyright infringement by a third party. Said person can be held liable for injunctive relief if the contributor has violated a reasonable duty of care to prevent such direct infringements. Contributory liability (Sec. 830 German Civil Code: Joint tortfeasors and persons involved) depends on the intent of the intermediary.

¹⁶⁰ Art. L.335-2-1 France IPC.

¹⁶¹ Arts 29 and 30, as well as 104 or 105 Brazilian Copyright Act.

¹⁶² Report Canada, citing *Bell Canada v. 1326030 Ontario Inc.* [iTVBox.net] and *Bell Canada v Lackman*, 2018 FCA 42 (CanLII), <<http://canlii.ca/t/hqj8w>> at para 35.

¹⁶³ *Ibid.*, citing *Bell Canada v. 1326030 Ontario Inc.* [iTVBox.net], 2016 FC 612 (CanLII), <<http://canlii.ca/t/gv257>>, and noting that at time of writing the trial had not yet been scheduled.

¹⁶⁴ Sec. 31 of the Thailand Copyright Act.

¹⁶⁵ Supreme Court, 13 February 2001, 55-1 Minshū 87 [*Tokimeki Memorial Case*]. The translation is available at <http://www.courts.go.jp/app/hanrei_en/detail?id=571>.

¹⁶⁶ See, respectively, Sec. 22(2) of the HK Ordinance; *CBS Songs Ltd v Amstrad Consumer Electronics Plc* [1988] RPC 567 at 578; and Sec. 273B(1) of the HK Ordinance.

of selling, producing, distributing, providing, or owning such device to facilitate “unlawful acts”; however, none of the acts specified in this law refers to copyright infringement.¹⁶⁷

For a Summary Table of the analysis in this subsection, please refer to ANNEX 3: Summary Tables Question 3 – online acts qualified as copyright infringement.

Other types of unauthorized use

The national experts did not report any significant other types of unauthorized online use of copyright-protected content not included in the activities described above.

Legal uncertainty areas

The analysis of primary liability in national laws uncovers three main drivers or areas of legal uncertainty: absence of case law on some activities; experiential use (passive streaming); and referential/mediated use (hyperlinking and sale of kodi boxes).

First, the absence of case law on many types of acts makes it hard to state with certainty whether they infringe copyright in some national laws. This is particularly true for acts like stream-ripping, passive streaming, hyperlinking and the sale of kodi boxes with unauthorized add-ons. In the EU, some of this judicial scarcity can be overcome to a certain degree by relying on the interpretative activity of the CJEU. In other jurisdictions, especially in Brazil and the Asian countries, it is only possible to rely on probability assessments by national experts. Therefore, some caution must be exercised before drawing sweeping judgments on the basis of the questionnaires.

Second, the legal qualification of passive streaming as a copyright-relevant act is unclear. In the EU, the issue appears to be settled after *Filmspelers*. However, outside Europe, it is noteworthy that some national laws do not consider this activity to merit copyright protection. This is grounded on the notion that passive streaming is *experiential* in nature, akin to the offline equivalent of reading a book or viewing a TV series. As such, streaming would not constitute a *use* of copyright in the legal sense.

Third, there is uncertainty in what we term “referential” or “mediated” use. This refers to types of acts, like hyperlinking and the sale of kodi boxes, that are: (1) in some countries *probably* governed by the right of communication to the public under a strict liability regime (Thailand and Hong Kong); (2) in EU national laws governed by the same right but subject to a knowledge test stemming from CJEU case law; and (3) in yet another set of laws governed by intermediary liability regimes (Canada, Brazil and Japan). Our main observation here is that for these acts there is a blurring of the lines between primary and secondary liability, with a significant degree of uncertainty as to the application of subjective elements in the assessment of the exclusive right of communication to the public.

Summary Table

For a Summary Table of the online acts qualified as copyright infringement across different national countries, please refer to ANNEX 3: Summary Tables Question 3 – online acts qualified as copyright infringement.

3.2. The relevance of different elements for infringement

¹⁶⁷ Report Indonesia, citing Art. 34(1) ITE Law and the remaining legislation.

When answering what types of acts qualify as online copyright infringement under their national laws, experts were asked about the relevance of different elements in making that assessment: (1) the knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content; (2) the commercial or for-profit nature or intent of the use or user; and (3) the type of protected content (music, audio-visual, books, and video games).

Regarding *knowledge* and *commerciality*, the main points to emphasize are those addressed above under the heading *areas of legal uncertainty*. In sum, other than the consideration of knowledge in the context of the legal qualification of downloading in Japanese law, the majority of acts described – from downloading to uploading – are strict liability torts. The situation differs when assessing the right of communication to the public in EU countries, and its application to hyperlinking and the sale of kodi boxes with pre-installed add-ons linking to unauthorized websites. In those cases, the subjective element of knowledge plays a central role in the legal qualification of the act. Furthermore, when assessing knowledge in that context, the CJEU has devised a rebuttable presumption that relies on the for-profit nature, character and/or intent of the linker, the precise contours of which are still in flux. Thus, in this context, the commercial nature or intent of the act plays an important role in the legal assessment of primary liability. The same can be said in Thailand as regards the application of the exclusive to the sale of kodi boxes with unauthorized add-ons.

Finally, as a rule, there appear to be no noteworthy differences for the assessment of primary liability depending on the *type of content* at issue, namely music, films and TV series, books, or video games. To be sure, the legal qualification of video games in national law as an independent work and/or as software was not clear in all questionnaires. However, this potential difference does not appear to affect the main conclusions regarding liability for the acts described above.

3.3. Liability of online intermediaries

The notion of “intermediary” and safe-harbors in national law

This section addresses the liability of online intermediaries. It discusses two interrelated questions. The first is how the different national laws approach the notion of “intermediary” in the context of copyright and whether there are relevant provisions that define specific types of intermediaries, such as ISPs, “hosting providers”, etc.¹⁶⁸ The second question is whether online intermediaries benefit from liability exemptions or safe harbors in national law and, if they do, what is their scope – i.e. the type of services covered and the conditions for application.¹⁶⁹

- EU

As noted, in EU law, the liability of intermediary service providers is partially harmonized by articles 12-15 of the ECD. The directive applies to “service providers” of “information society services” and includes conditional liability exemptions or safe harbors (regarding claims for damages) to the benefit of intermediaries concerning the provision of services of “mere conduit” (or access), “caching”, and “hosting”. For the purposes of copyright, these provisions should be read in conjunction with Article 8(3) InfoSoc Directive. For a description of both regimes and major lines of CJEU case law, see *supra* at 2.2.

All national laws implement the ECD’s concepts and safe harbors with varying degrees of detail. With the exception of Poland, all member states have also implemented Article 8(3) of the InfoSoc Directive. To the extent national laws follow the directive’s regime, we only highlight below the specificities of national legal systems on this topic.

¹⁶⁸ Annex 1: Legal Questionnaire, Question 2.

¹⁶⁹ Ibid., Question 5.

FRANCE

France has implemented the ECD and its safe harbor system (including the general prohibition on monitoring) in Article 6 of the LCEN and the Postal and Electronic Communications Code.¹⁷⁰ Both instruments define ISP, while the LCEN advances a definition of hosting providers as “a person or legal entity that stores, even without cost – for the provision of public services by public communication online – signals, texts, images, sounds or messages of any kind provided by the recipients of those services”.¹⁷¹ The definition includes user-upload content websites, such as YouTube, Dailymotion and Google, regarding the content uploaded by users.

ISP liability can only occur with respect to the information transmitted if they are at the source of the request for the transmission, if they select the recipient of the transmission, or if they select or modify the content that is the object of the transmission.¹⁷²

In general terms, *civil* liability for hosting providers arises where two conditions are met, stemming from Article 14 ECD. First, the provider has actual knowledge of (1) the unlawful nature of the hosted content or (2) of facts and circumstances showing that nature. Second, the provider fails to act promptly to remove data or block access to the content once that knowledge is obtained.¹⁷³ Actual knowledge may result from a notice of infringement from the copyright owner, which must contain certain elements established in the law. These include information on the applicant, the description of the litigious facts and their precise location (URL), the legal basis, and a record of the contacts (or attempts to contact) with the alleged infringer.¹⁷⁴ Upon receipt of the notice, the hosting provider must takedown the content promptly, i.e. in one or two days.

GERMANY

German law distinguishes between different types of intermediaries and different types of liability these may incur in. The relevant provisions can be found in the German Civil Code and the Tele-Media Act.

The German Civil Code contains two headings that may give rise to intermediary liability. The first is based on the concept of “interferer liability” (*Störerhaftung*),¹⁷⁵ a doctrine significantly shaped by case law.¹⁷⁶ An interferer is a person who has willfully made a causal contribution to the direct copyright infringement by a third party. Such an interferer can be held liable for injunctive relief (not damages) if it has violated a reasonable duty of care to prevent the direct infringement at stake. The doctrine applies to all types of intermediaries. The second heading is contributory liability.¹⁷⁷ Depending on the intent of the intermediary, joint tortfeasors and other persons involved in an infringement of copyright can be held liable. In most cases there is no finding of contributory liability due to the difficulty in establishing knowledge of the specific copyright infringement.

In addition, the relevant provisions of the ECD are implemented in Germany in the Tele-Media Act.¹⁷⁸ These provisions follow closely the directive’s template and are important when assessing interferer liability, as they are taken into account when considering if an intermediary violated a reasonable duty of care to prevent a direct copyright infringement. As a result, within the concept of

¹⁷⁰ Report France.

¹⁷¹ Art. 6-I-2 LCEN.

¹⁷² Art. L.32-3-3 of the Postal and Electronic Communications Code.

¹⁷³ Art. 6-I-2 LCEN.

¹⁷⁴ Art. 6-I-5 LCEN.

¹⁷⁵ Sec. 1004 German Civil Code.

¹⁷⁶ Report Germany.

¹⁷⁷ Sec. 830 German Civil Code.

¹⁷⁸ Secs 7-10 of the Tele-Media Act.

“interferer liability”, hosting and access providers only have to react if they have been informed about the infringement, leading in practice to an NTD system.¹⁷⁹

As we discuss below, some uncertainty exists in German law regarding the qualification of activities of certain intermediaries as regarding own content/use, in which case the provider is primarily liable and no safe harbor applies, and external content/use, where safe harbors may apply.¹⁸⁰

THE NETHERLANDS

Dutch law does not define the notion of “intermediary” specifically for copyright purposes. Instead, the Dutch Civil Code provides a general definition of a “service of the information society” similar to the ECD.¹⁸¹ This notion is understood as having the same meaning as “intermediary”.¹⁸² The Civil Code faithfully implements the directive’s provisions on safe harbors and no monitoring,¹⁸³ with the Criminal Code exempting providers of telecommunications services in comparable terms.¹⁸⁴

Although Dutch law does not include a statutory NTD procedure, intermediaries can be ordered to implement effective procedures of this type based on Article 6:196c of the Civil Code.¹⁸⁵ Based on this legal provision, several Dutch intermediaries have adopted voluntary NTD procedures under a Code of Conduct setting out how intermediaries are expected to respond to requests for removing content, including copyright infringing content.¹⁸⁶

POLAND

In Poland there are no specific provisions that define the notion of “intermediary” for purposes of copyright infringement. Notably, Poland has failed to implement Article 8(3) of the InfoSoc Directive, under which right holders may apply for injunctions against intermediaries whose services are used by a third party to infringe copyright (see *supra* at 2.2). The relevant provisions of the ECD are implemented in the Polish E-Commerce Act.¹⁸⁷

As the Polish expert rightly notes, safe harbors do not determine the liability of intermediaries. They merely provide exemptions from it. Therefore, the notions of intermediaries conceived for these purposes do not exhaust all possible “intermediaries” that could be held liable for copyright infringement.¹⁸⁸ In essence, the safe harbor regime in the Polish E-Commerce Act closely follows the directive, with three points of departure.

First, the no monitoring obligation appears to be broader in national law, as it applies to “all” monitoring and not just “general” monitoring.¹⁸⁹ Second, Polish law appears to require actual knowledge of the infringement, whereas the directive mentions also *awareness* of “facts or circumstances from which the illegal activity or information is apparent.”¹⁹⁰ Third, for hosting

¹⁷⁹ Report Germany.

¹⁸⁰ The distinction derives from the language in Sec. 7(1) of the Tele-Media Act.

¹⁸¹ Compare Art. 2(a) ECD with Art. 3:15d(3) of the Dutch Civil Code (“any service which is usually performed in exchange for a financial consideration, at or from a distance by electronic transmission, at the individual request of the consumer of the service, without parties having been simultaneously present at the same place. A service is performed electronically if it is sent out, transmitted and received exclusively by wire, by radio or by means of optical or other electromagnetic sources, using electronic equipment for the processing, including digital compression and the storage of data”).

¹⁸² Report Netherlands.

¹⁸³ Art. 6:196c Dutch Civil Code.

¹⁸⁴ Art. 54a Dutch Criminal Code.

¹⁸⁵ Appellate Court of Amsterdam 19 August 2014, ECLI:NL:GHAMS:2014:3435, NSE/Brein.

¹⁸⁶ See Gedragscode Notice-and-Take-Down, available at: <<https://ecp.nl/publicaties/ntd-gedragscode-nl/>>.

¹⁸⁷ Arts 12-15 of the Polish E-Commerce Act.

¹⁸⁸ Report Poland.

¹⁸⁹ Report Poland. There are however no court decisions on this.

¹⁹⁰ Report Poland, noting that some court decisions, including the judgment of the Supreme Court of September 30 2016, seem to disregard this discrepancy.

providers, national law only mentions an obligation to *disable access* to the illegal information, whereas the directive also mentions the *removal* of said information.

SPAIN

Spain has implemented the ECD through its Act 34/2002 (LSSICE),¹⁹¹ which broadly defines an ISP as anyone who provides an economic activity through the Internet or through any other telematic means.¹⁹² This definition encompasses ISPs that act as intermediaries in the transmission of content through telecommunication networks and benefit from safe harbors.¹⁹³

The LSSCIE distinguishes between four types of intermediary information society services: (1) mere conduit providers, (2) caching providers, (3) hosting providers, and (4) search engines/hyperlinks.¹⁹⁴ The first three categories were implemented almost verbatim from the directive, whereas the fourth category is a novelty, but follows the same conditions set for the hosting safe harbor.¹⁹⁵

In an illustrative example of this law's application, the Appellate Court of Madrid has classified YouTube as an intermediary hosting provider that may benefit from the application of the respective safe harbor. The court stated that the safe harbor should apply not only to web hosting services, but also to user-upload Web 2.0 websites, noting that YouTube was carrying out a "merely intermediary" activity, while downplaying any "editorial functions" of the service.¹⁹⁶

Regarding the safe harbor regime, a relevant difference is that, unlike the directive, Spanish law does not contain two knowledge standards: "actual knowledge" (for liability claims) and "awareness" (for damages). Instead, it refers solely to "actual knowledge", which has been interpreted as referring to knowledge obtained both by a court order and by other means, presumably a sufficiently detailed private notice system.¹⁹⁷

Spanish Copyright law includes two further notable idiosyncrasies. First, since 2014, there is a specific provision allocating liability for civil and, eventually, criminal copyright infringement to any ISP that: (1) knowingly "induces" the infringement; (2) knowingly "cooperates" with the infringement, or (3) having a direct economic interest in the infringement, has the power to control it.¹⁹⁸ As noted by the Spanish expert, these are the same instances "of secondary (indirect) liability (inducement, contributory infringement and vicarious liability) developed by U.S. copyright case law". The reason for the introduction of the provision – which might not have been warranted due to existence of general rules on liability applicable to intermediaries in the Civil Code – appears to have been the highly publicized *ManolitoP2P* judgment (2014) that absolved a website providing P2P software that could be used to access unlawfully posted content.¹⁹⁹ Notably, this provision does not affect the aforementioned safe harbors, provided their legal requirements are met.²⁰⁰ The second idiosyncrasy is the provision of a crime tailored for websites that offer links to infringing contents (on

¹⁹¹ Act 34/2002 on services of the information society and e-commerce (LSSICE).

¹⁹² NB the ECD definition of service provider is similarly broad. See Report Spain.

¹⁹³ Art. 1 LSSCIE. See Report Spain.

¹⁹⁴ Arts 14-17 LSSCIE.

¹⁹⁵ NB Art. 21(2) ECD considers as a possible future area of harmonization the "liability of providers of hyperlinks and location tool services".

¹⁹⁶ See Sent. JM n.7 Madrid, 20 Sept.2010; partially confirmed by AP Madrid (Sec. 28) January 14, 2014 [*Telecinco v. Youtube*] Westlaw.ES JUR/2014\36900.

¹⁹⁷ See SGAE v. Asociación de Internautas, STS (civil ch.) 9 December 2009. The safe harbor provisions have given rise to abundant case law regarding copyright infringement, in civil, criminal, and administrative jurisdictions. For an extensive list of cases (civil and criminal) on ISP liability in Spain, see Responsabilidad en internet – Blog by MIQUEL PEGUERA: <https://responsabilidadinternet.wordpress.com/>.

¹⁹⁸ Art. 138 TRLPI, as amended by Act 21/2014.

¹⁹⁹ Report Spain, making reference to the case AP Madrid (Sec. 28), 31 March 2014 [*ManolitoP2P*] Westlaw.ES AC/2014\652.

²⁰⁰ Report Spain.

P2P and other platforms), regardless of whether their activity qualifies as a copyright infringement or not.²⁰¹

SWEDEN

In Swedish law, the term “intermediary” is only mentioned in the Copyright Act’s implementation of Article 5(1) InfoSoc Directive, which exempts the making of temporary copies from the scope of the reproduction right.²⁰² The Act does not define that term or distinguish between types of intermediaries.²⁰³ Still, the Swedish implementation of the ECD, the E-Commerce Act, applies to “service providers”, i.e. “physical or legal persons that provide an information society service”, defined in similar terms to the directive.²⁰⁴ Intermediaries falling within this definition may be exempted from *financial* liability (compensatory damages or administrative penalties) for the transfer of infringing content, if their services benefit from one of the three traditional safe harbors: mere conduit service, caching, and hosting.²⁰⁵

As regards criminal liability, Swedish law contains a provision according to which “a service provider that transfers or stores information for another may be found liable for a crime relating to the contents of the information only if the crime has been conducted intentionally.”²⁰⁶ This provision has been applied, for example, to exclude the application of safe harbors to the operators of *The Pirate Bay* and convict them of criminal secondary liability for copyright infringement.²⁰⁷

Furthermore, Swedish law contains a “social benefit” (*social adekvans*) exception for civil and criminal liability arising from contributory acts that may apply to certain ISPs. According to this doctrine,

*A defendant may be absolved from liability under certain special circumstances if the act can be said to do more good than cause harm. Essentially, where an act involves conscious risk taking and produces a harmful effect, it may nevertheless be allowed on consideration of factors such as the type of risks, the values targeted by the risks, the social value of the act, and the precautionary measures which have been possible and justified.*²⁰⁸

The application of this “no liability” principle to ISPs was considered in the preparatory works to the national implementation of the ECD²⁰⁹ and developed in the aforementioned *The Pirate Bay* case, with the court ultimately deciding against the platform.²¹⁰ In this respect, the national expert notes that the principle at stake may have recently lost its relevance in cases involving intermediaries, as a 2017 decision from the Patent and Market Court of Appeals, concerning the first website blocking injunction against an ISP in Sweden, did *not* address the applicability of the principle at all.²¹¹

UK

²⁰¹ Report Spain, citing Art.270.2 Criminal Code (as amended in January 2015 by LO 1/2015).

²⁰² Art. 11a Swedish Copyright Act.

²⁰³ The preparatory works to the Copyright Act also fail to define the notion and only make a reference to recital 33 of the directive. The recital states that “a condition for temporary forms of copies to be exempted from the exclusive rights is that the intermediary does not modify the information and does not interfere with the lawful use of technology which is commonly recognized and which is used in the industry to obtain data about how the information is used”.

²⁰⁴ Art. 2 Swedish E-Commerce Act.

²⁰⁵ Arts 16-18 Swedish E-Commerce Act.

²⁰⁶ Art. 19 Swedish E-Commerce Act.

²⁰⁷ Case B 4041-09 (judgment delivered on 26 November 2010), Svea Court of Appeals.

²⁰⁸ Report Sweden: “social adekvans is a legal technical term but is often translated, somewhat erroneously, into social adequacy. For the sake of convenience it will be refer to as a principle, even though there is disagreement as to whether it ought to be categorised as a principle, exception or a “fail-safe”.”

²⁰⁹ Regeringens prop. 2001/02:150, pp. 89.

²¹⁰ Case B 4041-09 (judgment delivered on 26 November 2010), Svea Court of Appeals. See Report Sweden.

²¹¹ Report Sweden, citing PMT 11706-15, delivered on 13 February 2017.

UK law does not employ the notion of “intermediary” per se. However, the Electronic Commerce (EC Directive) Regulations 2002 refer to the term “information society service provider” in terms similar to the ECD, and contain near-identical safe harbor provisions for mere conduit, caching, and hosting services.²¹² The main difference to the directive’s wording is the clarification that the UK safe harbors “protect the service providers from any liability that might otherwise apply for damages or for any other pecuniary remedy or for any criminal sanction”.²¹³

- AMERICAS (BRAZIL, CANADA)

BRAZIL

The Brazilian Copyright Act does not contain express provisions on Internet intermediaries. However, a separate piece of legislation, the “Internet Civil Act” (*Marco Civil*), defines intermediaries as providers of “connection to internet” and of “internet applications”,²¹⁴ further setting out safe harbors for intermediaries. However, since the Act expressly excludes copyright from its scope of application, these safe harbors do not apply to copyright infringement.²¹⁵

In light of this exclusion, ISPs may be subject to contributory liability under the Copyright Act and the general rules of civil responsibility in the Civil Code and Consumer Rights Code.²¹⁶ Building on these provisions, the Superior Court of Justice has developed a tort law based secondary liability (or “subsidiary responsibility”) regime for hosting providers. This regime, as it currently stands, can be summarized as follows.²¹⁷

- If a hosting provider gains knowledge of the infringing content on its platform, it must quickly remove (takedown) the allegedly infringing content.
- Knowledge is normally obtained through private notice of the copyright owner, i.e a Court order is not required.
- The notice must be sufficiently detailed, identifying the content to be taken down and the exact URL where that content is found.
- The removal of the content must occur within a short time frame (e.g. in one case this amounted to 24 hours post notice). Failure to expeditiously remove the content gives rise to liability of the provider.
- The removal is temporary, allowing the service provider to examine the notice and make an assessment of the copyright infringing nature of the content.
- If the provider considers the content to be lawful, it may re-upload it. In making this assessment, one factor to consider is whether the use in question is covered by an exception to copyright.
- In determining the liability of a service provider, other relevant factors to consider are the primary function of the service provider in question (e.g. whether it is a file sharing platform or a social network), whether the failure to remove the content damaged the copyright owner, and whether the service provider profited from the copyright infringement by its third party user.

CANADA

Canadian law contains a general safe harbor for intermediaries. According to this, persons who only supply “the means of telecommunication necessary for another person to so communicate” are not

²¹² Secs 2(1) and 17-19 of the UK Electronic Commerce Regulations 2002.

²¹³ Report UK.

²¹⁴ Art. 5-VII Brazil Internet Civil Act defines “internet applications” as “a set of functionalities that can be accessed through a terminal connected to the Internet”. See also Arts 19 and 31 Brazil Internet Civil Act.

²¹⁵ Arts 19 and 31 Brazil Internet Civil Act. See Report Brazil.

²¹⁶ See Brazil Report, citing the relevant provisions.

²¹⁷ Report Brazil.

themselves to be considered parties to an infringing communication.²¹⁸ The meaning of telecommunication is interpreted broadly, including all “connection equipment, connectivity services, hosting and other facilities and services”,²¹⁹ and likely includes search engines.²²⁰

The Canadian Copyright Act contains safe harbors for intermediaries that codify a number of Supreme Court cases.²²¹ The safe harbors apply to “network services” (mere conduit), “incidental acts” (caching), and hosting services.²²² As a result, the Act shelters most Internet intermediaries, such as ISPs, hosting services, and search engines, from civil liability for copyright infringement by their users.²²³

The application of the safe harbors is subject, first, to the conditions typical for each type of service, such as neutrality (and non-interference) for caching services, and knowledge of the infringing nature of the stored content for hosting.²²⁴ In addition, for a safe harbor to apply, the act in question must not infringe a provision on so-called “enabler liability”,²²⁵ according to which

it is an infringement of copyright for a person, by means of the Internet or another digital network, to provide a service primarily for the purpose of enabling acts of copyright infringement if an actual infringement of copyright occurs by means of the Internet or another digital network as a result of the use of that service.”²²⁶

This provision can be used by copyright holders to attack Internet intermediary services such as *The Pirate Bay* or *Popcorn Time*, as occurred in a lawsuit filed by copyright holders against a provider of a BitTorrent search service.²²⁷ However, since that case was settled, Canadian courts have yet to interpret the provision.²²⁸

The Canadian Copyright Act also includes a special regime for providers of “information location tools”, i.e. any tool that makes it possible to locate information that is available through the Internet or another digital network. This term may encompass generic search engines and other ISPs, shielding them from damages.²²⁹ Subject to certain conditions, the copyright owner is only entitled to an *injunction* against a provider of an information location tool that is found to have infringed copyright by making a reproduction of the work or other subject-matter or by communicating that reproduction to the public by telecommunication.²³⁰

Furthermore, the safe harbor scheme includes since 2015 a notice-and-notice system.²³¹ According to this, a copyright owner can first send a notice to the ISP claiming infringement, which must include the IP address linked to the alleged infringement. The ISP will then locate the specific subscriber and relay the notice to the individual, without disclosing the personal information to the copyright

²¹⁸ Copyright Act (R.S.C., 1985, c. C-42), Sec. 2.4(1)(b). Added by S.C. 1997, c. 24, Sec. 2.

²¹⁹ 2004 SCC 45. [SOCAN], at 92.

²²⁰ Report Canada.

²²¹ The relevant sections are 31.1(1)-(2), (4) and 41.27(1) Canadian Copyright Act.

²²² See Sec. 31 Canadian Copyright Act.

²²³ Secs 2.4(1)(b), 31.1(1)-(2), (4) and 41.27(1) Canadian Copyright Act.

²²⁴ Secs 31.3 and 31.5 Canadian Copyright Act.

²²⁵ Sec. 31.1(6) Canadian Copyright Act: “Subsections (1), (2) and (4) do not apply in relation to an act that constitutes an infringement of copyright under subsection 27(2.3).”

²²⁶ Sec. 27(2.3) Canadian Copyright Act.

²²⁷ B.C. Sup. Ct. File No. S086309, settled on consent July 13, 2016.

²²⁸ NB: a similar provision exists that prohibits providing services or manufacturing technology primarily for the purposes of facilitating the circumvention of TPMs. See Sec. 41(1)(b)-(c) Canadian Copyright Act.

²²⁹ See <https://www.dentons.com/en/insights/articles/2017/april/12/first-judicial-consideration-of-information-location-tool-under-the-copyright-act>, commenting on *Trader Corporation v. CarGurus*, 2017 ONSC 1841.

²³⁰ Sec. 41.27 Canadian Copyright Act.

²³¹ Canada, Bill C-11, An Act to amend the Copyright Act, 1st Sess., 41st Parl, 2012, cl 47 (royal assent on 29th June 2012). A similar notice and notice scheme operated informally in Canada for many years before it was formalized through the 2012 amendments. See SOCAN at para. 110.

owner.²³² In this context, the intended role of the intermediary (the ISP) is to pass on the notice to subscribers. In the law, the intermediary is more specifically defined as the “person who provides the means, in the course of providing services related to the operation of the Internet or another digital network, of telecommunication through which the electronic location that is the subject of the claim of infringement is connected to the Internet or another digital network.”²³³ If the intermediary does not pass on the notice to the subscriber at the identified IP address they are subject to statutory damages, capped at \$ 10 thousand.²³⁴

Finally, the Canadian Copyright Act provides for an exception for “non-commercial user-generated content”.²³⁵ In the context of this exception, an intermediary is defined as “a person or entity who regularly provides space or means for works or other subject-matters to be enjoyed by the public”.²³⁶ In other words, hosting platforms are exempted from liability where the uploading act by their individual users is covered by the exception.

- ASIA (HONG KONG, INDONESIA, JAPAN, THAILAND)

HONG KONG

The Hong Kong Copyright Ordinance does not provide for definitions of intermediaries or intermediary services, or include intermediary specific safe harbors. Liability of intermediaries can be established under two headings: infringement by authorization²³⁷; and contributory infringement as a common law tort. Both headings “require a heavily fact-sensitive inquiry as to whether there are any measures in place to enforce the takedown of infringing contents, the main activities of the online intermediary etc.”²³⁸

INDONESIA

The law of Indonesia recognizes intermediaries as ISPs (including private and public enterprises) but does not advance a notion or differentiate between specific types of intermediaries. One legal instrument (the ITE Law) advances a definition of “electronic system provider” that applies to different services (dialup, DSL, cable, Wi-Fi access, and satellite), and regulates their operation and responsibility.²³⁹ The expert notes that it is debatable whether online intermediaries benefit from safe harbors, but they appear to be subject to liability on the basis of a duty of care principle stemming from Article 1367 of the Indonesia Civil Code.²⁴⁰

Although Indonesia has no specific legislation on liability of intermediaries, the activities of ISPs and other service providers are regulated by two Circular Letters of the Minister of Information and Communication. The first is *Circular Letter No. 3 Year 2016* concerning “Service Provider Application and/or Content through Internet (Over the Top)”, which inter alia regulates the obligation to obey laws on intellectual property rights, as well as the broadcasting and film regulation. The

²³² Secs 41.25 (notice of claimed infringement) and 41.26 (on obligations, fees and damages related to notices) Canadian Copyright Act.

²³³ Sec. 41.25(a) Canadian Copyright Act.

²³⁴ Sec. 41.26(3) Canadian Copyright Act.

²³⁵ Sec. 29.21 Canadian Copyright Act provides: “It is not an infringement of copyright for an individual to use an existing work or other subject-matter or copy of one, which has been published or otherwise made available to the public, in the creation of a new work or other subject-matter in which copyright subsists and for the individual” for non-commercial purposes.

²³⁶ Sec. 29.21(1) Canadian Copyright Act.

²³⁷ Sec. 22(2) HK Copyright Ordinance.

²³⁸ Report Hong Kong.

²³⁹ Report Indonesia, citing Arts 1(6), 15 and 16 ITE Law.

²⁴⁰ Report Indonesia. The provision reads, in the relevant part: “A person is responsible for the damage which was caused by his own act, as well as for that which was caused by the acts of the individuals for whom he is responsible, or caused by matters which are under his supervision. The above-mentioned responsibilities cease, if the parents, guardians, school teachers and work supervisors can prove that they were unable to prevent act, for which they would be liable.”

second is *Circular Letter No. 5 Year 2016* the “Limitation and Accountability of Trade Platform Provider through Electronic System (Electronic Commerce)”. This Circular prohibits publication of content that infringes intellectual property rights, and imposes certain obligations on platform providers, such as: to “determine the requirement of platform usage, including provisions regarding the responsibility of uploaded content”; to provide “embedded means” of reporting illegal content on the platform; and, upon reception of notice thereof, to remove or block access to the illegal content, including unauthorized copies of copyright works. If the service provider does not comply with this obligation, the Ministry of Communication and Information has the power to close the online platform.²⁴¹

JAPAN

The Japanese Copyright Act does not contain a definition of “intermediary” or an explicit legal basis for injunctive relief against a person who contributes to or supports an infringement. However, the Japanese ISP Liability Limitation Act limits the liability for damages of ISPs (hosting providers) for different types of infringement, including of copyright.²⁴²

Under this act, an ISP is exempted from liability for damages for copyright infringement caused by its “information distribution” unless two cumulative conditions are met. The first is that “it is technically possible to take measures for preventing such information from being transmitted to the public”. The second appears to translate as knowledge or awareness of the direct infringement occurring through its service.²⁴³ If the ISP “immediately acts upon the knowledge and removes the infringing content, it is not liable for damages under the ISP Liability Limitation Act.”²⁴⁴

THAILAND

Thailand’s national law defines “intermediary” as “service provider”. The latter can be “a service provider to others in accessing the internet or enabling others to contact one another by other means through a computer system whether the service provider does so under his name, or those of others or in the interests of others” or “a service provider for computer information storage for the interests of others”.²⁴⁵ The Copyright Act includes a safe harbor regime for service providers. According to this, if the provider (1) does not “control, initiate or command the infringement of the copyrighted material in their computer system” and (2) complies with a Court order against the infringing content, then it will be exempted from liability for damages related to the infringement.²⁴⁶

Legal uncertainty on intermediary or secondary liability

The section attempts to identify any uncertainty in national law as to whether some activities give rise to primary liability or benefit from safe harbors.²⁴⁷ The point here is to understand how national law draws the line between primary and secondary liability and distinguishes hard cases. This is particularly relevant in light of the expanding scope of exclusive rights in the digital environment and the regular calls for increased liability of Internet intermediaries, especially where these go beyond the mere provision of the services covered by safe harbors.

- EU

²⁴¹ Report Indonesia.

²⁴² Act No. 137 of November 30, 2001 (Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders).

²⁴³ Art. 3(2) ISP Liability Limitation Act.

²⁴⁴ Report Japan.

²⁴⁵ Sec. 32/3 Thailand Copyright Act and Sec. 3 of the Computer-Related Crime act.

²⁴⁶ Sec. 32/3 Thailand Copyright Act.

²⁴⁷ Annex 1: legal Questionnaire, Question 6.

Legal uncertainty has arisen to different degrees in the **majority of the Member States** as a result of CJEU case law on the right of communication to the public and on the safe harbors in the ECD. First, the broad interpretation of the right of communication to the public (including the introduction of a knowledge test in the context of the new public requirement) has extended its scope to activities such as the making available and management of online file sharing platforms.²⁴⁸ For hosting platforms, especially the ones with a hybrid character, CJEU case law raises uncertainty about when they can benefit from the ECD safe-harbor and when the activities are considered to be a communication to the public.

Also, as noted (*supra* at 2.2), CJEU rulings in cases like *L'Oréal/eBay*²⁴⁹ and *Google France/Louis Vuitton*²⁵⁰ have clarified that to benefit from safe harbors, the activity of intermediary hosting service providers must be predominantly “neutral”, in the sense that it is “of a mere technical, automatic and passive nature, so that the information society service provider has neither knowledge nor control over the information which is transmitted or stored”.²⁵¹ While the neutrality requirement does not appear to impose a requirement of absolute passivity from hosting providers, its application is difficult in practice and may generate uncertainty. It is further challenging for courts to determine when there is “actual knowledge” of the infringing activities. This notion, introduced by the ECD in connection with the caching and hosting safe harbors, has led to uncertainty in some national laws.²⁵² Finally, there is uncertainty in delineating what constitute admissible “specific” (and therefore admissible) monitoring obligations for intermediaries under Article 15 ECD.

German law echoes some of these challenges in its differentiation of service providers’ use of own information/content and external information/content (i.e. information of third parties).²⁵³ No safe-harbors apply with respect to own content, for which intermediaries shall be liable in accordance with general principles of direct liability. Regarding external content, on the other hand, intermediaries can benefit from safe harbors identical to those of the ECD. However, the line between own and external content/information is difficult to draw. According to the German Federal Court, content is to be considered as own content if the intermediary takes on responsibility for the content published on his website. That assessment is made on the facts of the case based on the perspective of an average user.²⁵⁴ In this respect, it is controversial whether material uploaded by users to YouTube qualifies as “own content”, giving rise to primary liability for the platform, or as third party content to be assessed under the principles of “interferer” liability.²⁵⁵

In Spain, the introduction in 2014 of new criteria for indirect liability²⁵⁶ – in effect a legal transplant from U.S. judge-made doctrines – has created uncertainty. In particular, the application of these criteria (contributory, vicarious and inducement liability) has not been tested in court, and it remains unclear how they articulate with existing safe harbors.²⁵⁷

In Sweden, it has not generally proven difficult for courts to determine whether an act falls within the safe harbor provisions or instead gives rise to primary liability. Any relevant difference between types of liability appears to simply concern the available remedies. However, the discussed CJEU judgments, namely *GS Media* and its progeny, might have the consequences of recasting as direct infringement many types of conduct traditionally qualified as secondary liability.

- AMERICAS (BRAZIL, CANADA)

²⁴⁸ CJEU, *Ziggo*.

²⁴⁹ CJEU, *L'Oréal/eBay*.

²⁵⁰ CJEU, *Google France/Louis Vuitton*.

²⁵¹ CJEU, *Google France/Louis Vuitton*, paras 112-114. See also CJEU: *L'Oréal/eBay*, paras 111-113; *Papasavvas*, paras 39, 41 and 45. NB: the CJEU develops this requirement on the basis of Recital 42 ECD.

²⁵² E.g. Report Spain.

²⁵³ Report Germany, see Sec. 7.1 Tele-Media Act.

²⁵⁴ BGH 12 November 2009, I ZR 166/07 Marionskochbuch.

²⁵⁵ Report Germany, citing OLG München, 28.1.2016 – 29 U 2798/15 – Allegro barbaro.

²⁵⁶ Report Spain. See Art. 138 TRLPI.

²⁵⁷ Report Spain.

BRAZIL

In Brazil, there is uncertainty on how an ISP can be held liable for copyright infringing acts of its users. Although primary liability is unlikely, an ISP may be subject to secondary and/or “subsidiary” liability. As noted, ISPs do not benefit from safe harbors in the Internet Civil Act, which expressly excludes copyright from its scope of application. In addition to this, the provisions in the Copyright Act on joint liability for contributions to infringing conduct appear inadequate to address intermediaries in practice. Against this background, courts have found support for holding ISPs liable on the basis of tort law provisions in the Civil Code and Consumer Rights Code.²⁵⁸

CANADA

In Canada, there appears to be no uncertainty as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe harbors. Despite that, we should point out the absence of case law on the application of the provision on enabler liability, which not only establishes liability for intermediaries, but operates as condition for the application of safe harbors.

- ASIA (HONG KONG, INDONESIA, JAPAN, THAILAND)

HONG KONG

Under Hong Kong law the extent of involvement required to establish liability of Internet intermediaries remains uncertain. The two main routes are (1) infringement by authorization²⁵⁹ and (2) contributory infringement as a common law tort. Both require a heavily fact-sensitive inquiry as to whether there are any measures in place to enforce the takedown of infringing content, what the main activities of the online intermediary are, etc. Due to the absence of case law and the limited guidance in the statute, there is uncertainty on the factors from which courts would infer authorization or contributory infringement, as well as the relative weight of each factor.

INDONESIA

The national expert for Indonesia did not make reference to any specific uncertainty in this regard, merely pointing to the fact that the liability of intermediaries derives from a general duty of care principle in the Civil Code and is mainly regulated by two Circular Letters of the Minister of Information and Communication, described in the previous subsection.

JAPAN

In Japan, the main uncertainty revolves around the legal status of video sharing platforms, which can be considered either primary infringers or ISPs benefiting from safe harbors. In this respect, the expert points to the *TV Break* case where the court granted an injunction and awarded damages against a video sharing platform, qualifying it as a primary infringer on the grounds that the service provider had incited the user’s uploading under its management with a profit purpose while neglecting to take down infringing video files uploaded to the platform.²⁶⁰

THAILAND

In Thailand, there is uncertainty as to whether a service provider can enjoy exemption for liability if it receives a court order based on Section 20 of the Computer-Related Crime Act for suppression of

²⁵⁸ Report Brazil.

²⁵⁹ Sec. 22(2) HK Ordinance.

²⁶⁰ IP High Court, 8 September 2010, 2115 Hanrei Jihō 102 [*TV Break Case*].

dissemination or removal of computer data which infringes copyright and constitutes a criminal act. It is not clear whether the safe harbors only apply to a damages claim based on civil law, since the Computer-Related Crime Act does not provide for safe harbor provisions.

3.4. Treatment of copyright infringement by minors

In this section we address whether the national laws of the investigated countries differentiate between acts of copyright infringement committed by minors and adults and, if so, what the relevant differences are.

- EU

In Europe, the liability of minors is partly a question of family law, an area that is yet to be harmonized due to the cultural differences among member states. The result is that national laws deal with this issue differently, typically outside copyright-specific legislation and within the remit of civil law. None of the member states investigated distinguishes between the civil liability of minors and adults in the sense that both can be held liable for copyright infringement. However, national laws diverge on who is considered liable for damages arising from infringement acts carried out by minors.

In **France** and **Spain**, liability for damages is attributed directly to the minor's parents or guardians.²⁶¹ In **the Netherlands**, conversely, parents or guardians may be held liable for infringing acts of minors in the following scenarios. They are liable for infringements by minors until the age of fourteen years old. Between the ages of fourteen and fifteen years old, the parents are liable unless they cannot be blamed for not preventing the minor's behavior; also, the minor himself can be blamed if he commits a "tortious act". From sixteen years of age onwards, the minor is liable if he commits a "tortious act".²⁶² The application of Dutch law can be illustrated with the case of a fifteen-year-old boy who managed and ran the website www.soccer4u.nl on which he published two photos of Johan Crujff without authorization and without attribution to the photographer. The court found the minor liable for damages and legal costs, but not the parents, as it is considered normal for a minor that age to run such a website without parent control. This meant the parents were not to blame for the infringing act. Furthermore, they were under no duty to specifically monitor their son's behavior in exploiting the website.²⁶³

In the **UK**, the expert notes that it is theoretically possible to exclude liability for damages to child-infringers on the grounds that the minor did not know, or had reason to believe, that s/he was committing an infringing act. However, no case has considered the matter.²⁶⁴

In **Sweden**, general tort law states that any person under the age of 18 that causes harm to another shall compensate the harm "to the extent it is reasonable, having regard to their age, development, nature of the act, existence of liability insurance and other economic relationships and other factors".²⁶⁵ Differently from other member states, Swedish law does not appear to attribute the minor's liability for copyright infringement to the parents/guardians.²⁶⁶

In **Germany**, minors that have not reached the age of seven cannot be held liable for copyright infringement. However, between the ages of seven and eighteen minors can be held liable provided

²⁶¹ Reports France and Spain.

²⁶² Report Netherlands, citing Art. 6:169 of the Dutch Civil Code.

²⁶³ Report Netherlands, citing District Court 's-Hertogenbosch, 2 October 2008, ECLI:NL:RBSHE:2008:BF9979, and District Court 's-Hertogenbosch, 3 September 2009, ECLI:NL:RBSHE:2009:BJ7462.

²⁶⁴ Report UK, citing Sec. 97(1) CPA.

²⁶⁵ Report Sweden, citing Ch. 2, para. 4 of the Skadeståndslag (1972:207) (Torts Liability Act), which compliments the Copyright Act in relation to certain remedies.

²⁶⁶ Report Sweden, citing Ch. 3, para. 5 Torts Liability Act.

they “have the insight required to recognize” such responsibility.²⁶⁷ Whatever liability the minor incurs it is directly attributed to the person with a duty to supervise him, typically the parents.²⁶⁸ In the 2012 *Morpheus* decision, the German Federal Court stated that although parents must explain copyright law to their children, they have no obligation to monitor their Internet use.²⁶⁹

Finally, in **Poland**, the general rules on liability of minors dictate that only persons from the age of thirteen can be held liable for a tort. In this event, liability can be attributed to the parents or legal guardians due to lack of supervision.²⁷⁰

Most experts did not mention the issue of *criminal liability of minors* for copyright infringement. Therefore, in this respect, we can only report for the situation in France and Sweden. In France, there is no minimum age set by law to incur in criminal liability. The judge must assess the minor’s discernment on a case-by-case basis and the type of sanction imposed will depend on the age of the minor.²⁷¹ In Sweden, criminal liability can only arise as from the age of 15.²⁷²

- AMERICAS (BRAZIL, CANADA)

The laws of Brazil and Canada do not differentiate between acts of copyright infringement by minors and adults for purposes of civil liability. However, under Brazilian law, *criminal* liability depends on the minor’s age, with different (increasing) degrees of sanctions.²⁷³

- ASIA (HONG KONG, INDONESIA, JAPAN, THAILAND)

The laws of Hong Kong, Japan and Thailand do not differentiate between acts of copyright infringement by minors and adults for purposes of civil liability. However, in Thailand, *criminal* liability for minors (persons under the age of twenty) varies according to his/her age.²⁷⁴ Other than that, the law of Indonesia specifies that that parents and guardians are responsible for the damage caused by minors who live with them under their supervision and authority.²⁷⁵ Furthermore, the settlement of cases of copyright infringement by minors is processed in the special juvenile court and by adults in the district court.²⁷⁶

4. Enforcement measures, procedures, remedies, and sanctions

This section aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (like warnings), or criminal (such as prison sentences). Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement include the following.²⁷⁷

²⁶⁷ Sec. 828 German Civil Code.

²⁶⁸ Sec. 832 German Civil Code.

²⁶⁹ BGH 15 November 2012, I ZR 74/12, *Morpheus*.

²⁷⁰ Report Poland.

²⁷¹ Report France.

²⁷² Report Sweden, citing Ch. 1, para. 6 Penal Code.

²⁷³ E.g., younger than 12 years old, between 12 and 15, and from 16 to 18 years old.

²⁷⁴ Secs 73-76 Thailand Penal Code. Minors that have not reached the age of 11 cannot be punished. Minors between the age of 11 and 15 cannot be punished either, but the Court may provide for an additional injunction. The punishment for minors between 15 and 18 years may be waived (at the court’s discretion) or reduced by half. Minors between the ages of 18 and 20 years old can only be punished if the punishment is reduced by one-third or half.

²⁷⁵ Report Indonesia, citing 1367 Civil Code.

²⁷⁶ Report Indonesia.

²⁷⁷ The examples listed here are taken from C. Angelopoulos, “European Intermediary Liability in Copyright” (Kluwer Law International 2016), pp. 465 et seq.

- The suspension from the Internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.
- The monitoring or filtering of content. In this context, “filtering” is defined as monitoring measures with the objective of identifying unwanted content for subsequent blocking, removal or disposal.²⁷⁸
- The blocking and removing of infringing content, including NTD.²⁷⁹ In this context, “blocking” is defined as the disabling of access for the intermediary’s users to undesirable content. Blocking may take place at the point which the data is requested or at that at which it is sent; it may involve specifically identified communications, user accounts or entire websites. For search-engines, blocking is carried-out by “de-indexing”.²⁸⁰
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary’s services cannot be used for its commission.²⁸¹
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- Graduated response systems, meaning systems where ISPs monitor subscribers’ potential illegal actions or act upon notification thereof, serving notices and warnings to subscribers to cease infringement. If users continue their practices after a number of warnings, sanctions are applied (e.g. suspension and termination of service, capping of bandwidth, and blocking of sites).²⁸²

Against this background, the section examines the responses to questions by experts on enforcement measures against users (4.1) and intermediaries (4.2), differences in public and private enforcement per content type (4.3), disclosure of personal data in the context of enforcement (4.4), entitlement to apply for enforcement measures (4.5), and most used and effective enforcement measures (4.6).²⁸³

4.1. Enforcement measures available against users

This subsection addresses the civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions available under national laws to address online copyright infringement by users, whether individuals or websites/platforms. In other words, if a certain act is qualified as direct infringement and gives rise to primary liability, what enforcement measures may apply to the person or entity committing the act? When answering this question, national experts were asked to note any differences that may apply depending on the type of protected content, namely music, audio-visual, books, and video games.

Civil

- EU

As noted (*supra* at 2.2), the Enforcement Directive harmonizes civil enforcement of intellectual property rights in the EU, including copyright. These measures include different types of injunctive relief and damages. All member states have implemented the directive and its provisions, with varying degrees of detail. To the extent national EU laws follow the directive’s regime, we will only highlight below the specificities of national legal systems on this topic. It should also be noted, as a

²⁷⁸ See Annex 1: Legal Questionnaire, Definitions.

²⁷⁹ For example, Art. 14 ECD includes the basis of an NTD system in the hosting safe harbor.

²⁸⁰ Annex 1: Legal Questionnaire, Definitions.

²⁸¹ For instance, the notices can be posted on the Intermediary’s terms and conditions, on the front-page of the platform, as a pop-up message for users of platform, etc. Cf. Angelopoulos 2016, op. cit., pp. 477–478.

²⁸² Annex 1: Legal Questionnaire, Definitions.

²⁸³ See Annex 1: Legal Questionnaire, Questions 7 to 13.

general remark, that punitive and statutory damages do not appear to be available for copyright infringement in any of the member states' laws.²⁸⁴

FRANCE

French law has a broad range of available enforcement measures, including infringement seizure, customs detention of goods at the request of the copyright holder, protective measures (in the pre-trial stage, such as blocking of bank accounts and other assets), damages, confiscation of proceeds made from the infringement of copyright (*in addition* to damages), confiscation and publicity.²⁸⁵ To calculate damages it is possible to take into account the negative economic consequences of the infringement, the moral prejudice caused to the right holder, and the infringer's profits. However, since the assessment of prejudice may be difficult, the court may *alternatively* award damages as a lump sum up to the amount of royalties due for a hypothetical license fee.²⁸⁶

GERMANY

German law likewise includes a broad range of available enforcement measures, including the right to require cessation of infringement (injunctions), different types of damages (including compensation for non-pecuniary damages), a right of information, claims for destruction, measures to recall and release of copies, publication of judgment, etc.²⁸⁷

Two important features of German law should be pointed out. First, a provision allowing defendants that immediately acknowledge the claim to not bear the costs of legal proceedings, thus incentivizing plaintiffs to first attempt to settle claims extra judicially.²⁸⁸ Second, the detailed "notification" regime set out in the Copyright Act for the right to require cessation (enforced by an injunction) of infringement, which imposes an obligation on the plaintiff of sending a "cease-and-desist" letter to the direct or indirect infringer before instituting judicial proceedings.²⁸⁹

NETHERLANDS

In the Netherlands, a copyright holder can avail himself of substantive proceedings, preliminary relief proceedings, or ex parte proceedings against copyright infringement by users. Ex parte injunctions are available in the context of preliminary relief proceedings where a plaintiff copyright holder shows that a delay would cause him/her irreparable damage. The decision is immediate and provisionally enforceable.²⁹⁰ No other remedies are available in ex parte proceedings. Differently, a wide range of measures are available in substantive and preliminary relief proceedings, subject to specific requirements.²⁹¹ These include injunctions (to stop the infringement) and monetary damages, the surrender of infringer's profits (*in addition* to damages) or monies obtained as result of the infringement, a right of information, publication of judgment, and recovery of reasonable attorney fees.²⁹²

POLAND

²⁸⁴ Two caveats should be made in this respect. First, "punitive" damages are understood here to exclude damages for moral prejudice, which most member states recognize. Second, with the exception of the report for Sweden, this point is not addressed expressly by the experts, but can be deduced from their answers.

²⁸⁵ Report France.

²⁸⁶ Report France, citing L.331-1-3 para. 2 France IPC, and noting that this amount is not exclusive of compensation for the moral prejudice caused to the infringer.

²⁸⁷ Report Germany.

²⁸⁸ Report Germany, citing Sec. 93 Code of Civil Procedure.

²⁸⁹ Sec. 97a German Copyright Act.

²⁹⁰ Report Netherlands, citing Art. 1019e Code of Civil Procedure. NB: no other remedies are available in ex parte proceedings.

²⁹¹ See Report Netherlands, pointing out that in preliminary relief proceedings a separate urgent interest is required for claiming damages and ancillary claims.

²⁹² Arts 27a, 28(2)(b), 28(9), and 28(10) Dutch Copyright Act and Art. 1019h Dutch Code of Civil Procedure.

Under Polish law, primary infringers are subject to general sanctions for copyright infringement (i.e. not specific to the online environment). These include: preliminary injunctions; general injunctions (to cease infringement or refrain from future infringement); damages (under general civil law, i.e. actual damage and lost profits, or as a double license fee, in which case fault is not required); restitution of profits; removal of the effects of the infringement; and information claims.²⁹³

SPAIN

Spanish law provides the following enforcement measures: injunctions, precautionary measures for immediate protection (also available against intermediaries), and damages.

Injunctions cover “restraining orders” specifically envisioned for the online environment. These include suspending the infringing exploitation and prohibiting the infringer from resuming it; seizing or sealing any equipment used for the unauthorized communication to the public of works; and suspending Internet services to any person who uses them to infringe copyright. These measures will include blocking access to and removing copyright infringing content.²⁹⁴ Measures to identify the alleged infringer can also take the form of injunctions to an ISP requesting the personal information of the infringer; these may be ordered by civil courts in “special cases”.

Precautionary measures are available for civil and criminal copyright enforcement, provided there is a preliminary assessment in favor of the claimant *and* there are reasonable grounds to fear infringement is imminent and effective protection requires these measures. Pre-trial discovery may also be granted to the author.²⁹⁵

Damages may be claimed for any economic and/or moral prejudice caused by an infringement. The economic damages may be calculated on the basis of lost profits/economic loss or the hypothetical license fee, with the possibility to add the damages for moral prejudice to this amount (following the CJEU judgment in *Liffers*).²⁹⁶

SWEDEN

Swedish law provides for the following civil enforcement measures: general injunctions; damages; special injunctions for the provision of information²⁹⁷; special injunctions for publication of judgments; recall, change or destruction of property or means used to infringe; investigation and preservation of evidence measures (applicable also to intermediaries).²⁹⁸

The general injunction provisions are flexible enough to accommodate different types of measures for preventing or reacting to copyright infringement, including interim and preliminary injunctions (subject to the requirements of probability of infringement and reasonable risk of harm to the exclusive right).²⁹⁹

Regarding damages, copyright is a strict liability tort. Direct infringement without intent gives rise to an obligation to pay damages as “equitable remuneration”. However, if the infringement is intentional or negligent, the infringer must pay *compensatory* damages. For the calculation of the latter damages the law takes into account factors like: lost profits, unjust enrichment (infringer’s profits); reputation harm for the protected content; non-economic harm; and the interests of the harmed parties.

²⁹³ See Report Poland.

²⁹⁴ Report Spain, citing Art. 139 TRLPI.

²⁹⁵ Ibid., citing Art. 143 TRLPI and Arts 728 et seq. LEC (“The granting of precautionary measures will be done according to the general rules of civil and criminal procedure”).

²⁹⁶ Ibid., citing Art. 140 TRLPI and CJEU, *Liffers*.

²⁹⁷ Sec. 53c Swedish Copyright Act. See Report Sweden and *infra* at 4.4.

²⁹⁸ Report Sweden, citing Secs 53b, 53c, 53e, 53h, 55, 56a to 56h Swedish Copyright Act.

²⁹⁹ Ibid., citing Sec. 53b Swedish Copyright Act.

Importantly, the copyright's act provisions on damages only apply to private copying from unlawful/unauthorized sources if the same was made with knowledge (intention) or gross negligence.³⁰⁰

UK

In general, UK law provides several remedies for claimants for the infringement of their copyright: damages; injunctions; accounts, etc.³⁰¹

Damages are not available where, at the time of infringement, the defendant did not know or had reason to believe that copyright subsisted in the work to which the action relates.³⁰² Differently, additional damages may be awarded if required by the circumstances, taking into account factors like the "flagrancy of the infringement" or the profits made by the infringer.³⁰³ In alternative to damages, claimants may opt for an account of profits, an equitable remedy (awarded at the court's discretion) that deprives the defendant of profits made from their infringement.³⁰⁴

Injunctions can be interim and final. Final injunctions are discretionary measures that may be granted to copyright owners that prove at trial the infringement of their rights by the defendant. Interim injunctions are granted if the matter is urgent or if it is otherwise desirable in the interests of justice. In copyright cases, the general approach is to first assess the seriousness of the matter and subsequently the fairness in granting an injunction. Factors considering when assessing the latter are the adequacy of damages as an alternative remedy, the balance of convenience, and the merits of the case.³⁰⁵

A particularly important injunction developed by English courts to preserve evidence prior to trial in copyright infringement cases is the "Anton Piller" order,³⁰⁶ since re-named "search order".³⁰⁷ Subject to strict requirements, this order allows a claimant to inspect the defendant's premises and to seize or copy any information that is relevant to the alleged infringement.³⁰⁸ The search order may be combined with a "freezing" or "asset preservation" order for the retention of property pending the outcome of litigation.³⁰⁹

- AMERICAS (BRAZIL AND CANADA)

BRAZIL

Brazilian law provides for injunctions and damages for civil copyright infringement.³¹⁰ Since the law has not been adapted to the specificities of online use – both as regards substance and enforcement measures –, its application to the online infringement must be done by analogy.

Through that process of legal interpretation there seems to be sufficient flexibility in the law to accommodate injunctions and coercive fines against individuals or online platforms (e.g. *The Pirate*

³⁰⁰ Ibid., citing Sec. 54 Swedish Copyright Act.

³⁰¹ Report UK, citing Sec. 96(2) CPDA. Other available remedies, such as delivery up and the right to seize infringing copies require tangible copies of protected works and are therefore not usually relevant to online infringement. See Secs 99 and 100 CPDA.

³⁰² Ibid., citing Sec. 97(1) CPDA.

³⁰³ Ibid., citing Sec. 97(2) CPDA.

³⁰⁴ Ibid.

³⁰⁵ Ibid, citing the leading case *American Cyanamid v Ethicon* ([1975] AC 396).

³⁰⁶ *Anton Piller v Manufacturing Processes* [1976] Ch 55.

³⁰⁷ Civil Procedure Act (CPA) 1997, Sec. 7; Civil Procedure Rules (CPR) Practice Direction 25A.

³⁰⁸ Report UK, further describing the requirements of a strong prima facie case, seriousness of the potential damage, incriminating evidence against defendant and the possibility that evidence is destroyed.

³⁰⁹ UK, citing CPR, r. 25.1(1)(f). This was formerly known as a "Mareva injunction".

³¹⁰ Report Brazil, citing Arts 102 to 110 Brazil Copyright Act.

Bay) making available works without the permission of right holders, or to order the destruction of equipment used to host unauthorized copies of works, such as computer devices.³¹¹

Regarding damages, the general rule is that the unauthorized publication (online: making available) of a copy of a work shall entitle the claimant to the payment of the price at which the copy would have been sold. Where the number of copies is unknown, the law refers to a statutory amount of three thousand. According to the national expert, in the application of this provision to an online scenario a reference would be made to the total number of copies. However, where damages are disproportionately large, they would have to be adjusted to a proportionate amount. In this respect, the expert labels this regime as a “presumed attribution of damages”.

Finally, there is a recent trend in the case law to consider ISPs jointly liable (“co-responsible”) for infringement if it fails to take down content subsequent to a notice. This qualification appears to reinforce the NTD system put in place by copyright holders and ISPs, and endorsed/modulated by case law from the Superior Court of Justice (see *supra* at 3.3 and *infra* at 4.2). This trend, however, cannot be considered definitive yet.³¹²

CANADA

Canadian law imposes civil liability on users that (1) infringe copyright and (2) circumvent TPMs. Under the first heading, copyright holders are entitled to the remedies available in law for infringement of a right, including injunctions, damages, and accounts.³¹³ Owners may elect to recover statutory damages *in lieu* of actual damages. Statutory damages are capped: for commercial infringements at \$20 thousand; for non-commercial infringements at \$5 thousand.³¹⁴

Under the second heading copyright owners are entitled to the full range of remedies available in infringement proceedings, with the exception of statutory damages against individuals who circumvented TPMs for their own private purposes.³¹⁵

• ASIA (HONG KONG, INDONESIA, JAPAN, THAILAND)

HONG KONG

The law of Hong Kong provides the following civil remedies aimed at direct infringers: injunctions (e.g. takedown orders); damages; account of profits.³¹⁶ Among the injunctions available is a Norwich Pharmacal order for disclosure of personal data of alleged infringers by intermediaries (see *infra* at 4.4).

Two aspects regarding rules on damages are identical to UK law. First, damages are not available against defendants that did not know nor had reason to believe that copyright subsisted in the work to which the action relates. Second, additional damages may be awarded if required by the circumstances, taking into account factors like the “flagrancy of the infringement” or the profits made by the infringer. A third factor specific to Hong Kong law is the “completeness, accuracy and reliability of the defendant’s business accounts and records.”³¹⁷

INDONESIA

³¹¹ Ibid., citing Arts 105 and 106 Brazil Copyright Act.

³¹² Ibid.

³¹³ Sec. 34(1) Canadian Copyright Act.

³¹⁴ Sec. 38.1(1) Canadian Copyright Act.

³¹⁵ Report Canada, citing Sec. 41.1(1)(a) Canadian Copyright Act.

³¹⁶ Report Hong Kong, citing Secs 107 and 108 HK Ordinance.

³¹⁷ Sec. 108 HK Ordinance. See also *supra* in this section 4.1 – Civil – EU – UK.

Indonesian law allows copyright holders to apply for civil remedies of injunctions and damages. In particular, the Copyright Act provides for injunctions to stop the infringing action.³¹⁸ Furthermore, Indonesian law allows for “Anton Pillar” orders, which are applicable also to cases of online copyright infringement (such orders are similarly allowed in the UK as “search orders”). Injunctions are issued by the Commercial Court. Finally, the Copyright Act provides for a process of “proof of evidence” by using electronic information and/or electronic documents.³¹⁹

JAPAN

Japanese law recognizes injunctive relief for copyright owners against primary infringers in the Copyright Act and the possibility of claiming damages for intentional or negligent copyright infringement in the Civil Code.³²⁰

THAILAND

The copyright law of Thailand does not deal specifically with civil enforcement measures. Thus, copyright owners avail themselves of the general measures available in the Civil and Commercial Codes, namely injunctions and claims for damages against acts of direct copyright infringement.³²¹

Administrative

- EU

Only the laws of France and the UK contain specific administrative enforcement measures against direct copyright infringement by users. In addition, Spanish law contains a special administrative procedure directed at ISP that can be considered to apply both to “users” and “intermediaries”, depending on how these concepts are defined.

FRANCE

French law contains different types of administrative measures. With relevance to online copyright infringement, the most relevant is France’s famous graduate response system. This system is partly administrative and partly criminal, since users may be condemned to the payment of fines.

The system was created with the objective of stopping the use of Internet access connections for infringing purposes. It has been highly controversial. As a result, it has been modified several times since its inception. The administrative authority created to implement the system is the High Authority for the Distribution of Works and the Protection of Rights on the Internet (HADOPI).

According to the law, a person with Internet access has an obligation to ensure that his connection is not used for copyright infringement.³²² Until a legal change in 2013, a violation of this obligation could lead to suspension of Internet access of the account in question.³²³ After this change, this is no longer possible and the applicable sanction is a fine of up to €1.5 thousand.

There are three cumulative conditions for the application of this sanction. First, the account holder whose connection was used for copyright infringement failed to secure his Internet access in a way that prevented the infringement (e.g. by restricting third party access to the Wi-Fi) or was not diligent in implementing means to secure access. Second, he was notified by letter or email to implement such

³¹⁸ Art. 106 Indonesia Copyright Act.

³¹⁹ Report Indonesia, citing Art. 111 Indonesia Copyright Act.

³²⁰ Report Japan, citing Art. 112(1) Japan Copyright Act and Art. 709 Japan Civil Code.

³²¹ Report Thailand.

³²² Art. L.336-3 France IPC.

³²³ The relevant change was enacted by Decree No. 2013-596 of 8 July 2013.

means by the competent entity (i.e. HADOPI's *Commission de protection des droits*).³²⁴ Third, his Internet connection was used for copyright infringement in the year following the notification. A final aspect is that ISPs are legally required to inform their subscribers in the services contract about the graduated response system and the means to secure their access to the internet.³²⁵

UK

In 2010, the UK adopted the “Digital Economy Act 2010” (DEA 2010), which introduced a graduated response system for the online enforcement of copyright. This system would work as follows. Upon notice by the copyright owner, ISPs would notify their subscriber whose IP address was connected to the infringement. Subscribers with a certain number of notifications would be added to a “copyright infringement list”, to be made available to copyright holders for purposes of further action against the subscriber. The regulator (OFCOM) would establish an “obligations code” governing both the notifications and their effects, namely the disconnection to the Internet of the infringer.³²⁶

The controversy surrounding system prevented its adoption. In the meantime, the UK government had manifested a preference for a voluntary scheme: the Voluntary Copyright Alert Programme (VCAP). This system, modeled on the US “copyright alert system”, was agreed in 2014 between the film and music industries, as well as four large ISPs. In simple terms, the VCAP involves agents of copyright owners sending evidence of copyright infringement to ISPs, which then send letters or alerts to infringing customers with the intent to discourage infringement. (To this point, the system is similar to the Canadian notice-and-notice approach discussed supra.) Under the VCAP, a maximum of four letters with language escalating in severity can be sent to a single IP address. No sanctions are admitted under the system, but copyright holders are free to pursue legal action against the individuals.³²⁷ The first letters were sent to subscribers in early 2017.³²⁸

SPAIN: SPECIAL ADMINISTRATIVE PROCEDURE

Finally, Spanish law introduced in 2011 a special administrative injunction procedure by the Intellectual Property Commission or CPI (sec. 2) against infringements done for commercial purposes by ISP. The procedure, reinforced and enlarged in 2004, may be understood as applying both to users and intermediaries.³²⁹ This is because it covers not only categories of intermediaries that traditionally benefit from safe harbours (e.g. pure hosting) but also websites that may be qualified as directly infringing copyright, depending on the specific case. The latter include user-generated content websites and those providing links to infringing contents, which may for example directly infringe upon the right of communication to the public. Where the procedure applies the latter type of website, it may be considered as targeting also “users” (*lato sensu*). Measures available under this procedure include the suspension of the Internet service provided to the infringer, blocking and removing infringing contents, and publication of notices regarding the infringement.³³⁰ For further details on the procedure and its application to intermediaries, see *infra* at 4.2.

• AMERICAS (BRAZIL AND CANADA)

³²⁴ This is the competent committee under Art. L.331-25 France IPC.

³²⁵ Report France, citing Art. 6-I-1 of the Act of 21 June 2004.

³²⁶ Report UK, citing Secs 3 to 7 DEA 2010.

³²⁷ Report UK, citing https://wiki.openrightsgroup.org/wiki/Voluntary_copyright_alert_programme.

³²⁸ ISP Review, ‘UPDATE2 UK ISPs to Send First Internet Piracy Warning Letters this Month’, 10 January 2017, available at: <http://www.ispreview.co.uk/index.php/2017/01/big-uk-isps-send-first-internet-piracy-warning-letters-month.html>.

³²⁹ The procedure was created by Act 2/2011, of March 4, on Sustainable Economy (LES). It was reinforced and enlarged by Act 21/2014.

³³⁰ Report Spain, citing <https://www.mecd.gob.es/cultura-mecd/areas-cultura/propiedadintelectual/lucha-contra-la-pirateria/marco-juridico/via-administrativa.html>.

The law of **Brazil** does not contain any specific administrative enforcement measures against direct copyright infringement by users. **Canadian** law, on the other hand, contains a separate provision on statutory damages for non-payment of royalties where the Copyright Board has approved a tariff.³³¹ However, this is not of particular relevance for online copyright infringement.

ASIA (HONG KONG, INDONESIA, JAPAN, THAILAND)

The laws of **Hong Kong** and **Japan** do not contain any specific administrative enforcement measures against direct copyright infringement by users.

INDONESIA

In Indonesia, administrative procedure is governed by the Joint Regulation of Minister of Law and Human Rights (No 14 Year 2015) and Minister of Communication and Information (No 26 Year 2015), based on authority granted by Article 55 of the Copyright Act. The Joint Regulation contains a procedure for complaints related to online copyright infringement reported to either of the two Ministries mentioned, directly or through an electronic system on the website of the competent authority (the Directorate General of Informatics or DGIP). Complaints can be submitted by copyright holders, licensees or CMOs. Administratively, a verification team at the Ministry of Communication and Information goes through the reports and provides recommendations to the DGIP. Decisions can be made to partly or entirely block access to infringing content. The Joint Regulation provides specific for time limits for this procedure and for the existence of a database of blocked sites/users.³³²

In addition, under the aforementioned *Circular Letter No. 5 Year 2016* (*supra* at 3.3) – an operational instrument of the ITE Law (and not the Copyright Act) –, user-generated content platform providers have an obligation to provide a reporting instrument for complaints regarding inter alia copyright infringing content they host, which instrument must allow identification of a specific link to that content. If sufficient evidence is provided with the notice/complaint, platform providers must take necessary action to remove the content or block access thereto.

THAILAND

In Thailand, the Computer-Related Crime Act provides for an administrative enforcement measure in case of copyright infringement that constitutes a crime. The Court can, by a petition of the competent officer with approval of the Minister, order the suppression of dissemination or removal “of computers which is a copyright infringement from a computer system”.³³³ In essence, this provision grants broad authority for officials with approval from the Minister to “file petitions for writs to stop dissemination of information, or to order the deletion of data from systems”³³⁴ where, for our purposes, the information or data in question qualify as criminal copyright infringement.

If the copyright infringement “bears characteristics which are contrary to peace and order or good morals”, a separate procedure applies. This procedure requires the intervention of a “Computer Data Screening Committee” prior to the Minister’s approval.³³⁵ The Committee, appointed by the Minister, is competent to define what content is included in this category and therefore to which this provision applies.³³⁶

³³¹ Report Canada, citing Sec. 38(4) Canadian Copyright Act.

³³² See IP Komodo, *Implementing regulation for online Takedown and Website Blocking in Indonesia* (20 August 2015), available at: <http://ipkomododragon.blogspot.nl/search/label/Indonesia%20copyright?updated-max=2015-09-09T23:58:00-07:00&max-results=20&start=10&by-date=false>.

³³³ Sec. 20 Computer-Related Crime Act. NB: the petition can be electronic.

³³⁴ ARTICLE 19, *Thailand: Computer Crime Act, 2017: Legal Analysis*, available at <https://www.article19.org/resources/thailand-computer-crime-act/>, p. 22 (labeling this as a “gag order” provision).

³³⁵ Sec. 20(2) Computer-Related Crime Act.

³³⁶ ARTICLE 19, *Thailand: Computer Crime Act, 2017: Legal Analysis*, available at <https://www.article19.org/resources/thailand-computer-crime-act/>, p. 22.

In both cases, this power is quite broad in scope, allowing the competent/authorized officers to compel the removal or suppression in question, or to do it “themselves”.³³⁷ Users that do not comply with the court order are subject to a fine (capped at 200 thousand Baht) and a further daily fine (capped at 5 thousand Baht) until corrective action is taken.³³⁸

Criminal

- EU

As noted, criminal enforcement measures are not harmonized in EU law.

FRANCE

Under French criminal law, courts will determine the sanction based on the nature of the offence and on the specific circumstances of the case (Article 132-24 of the Criminal Code). The French IPC lists the available criminal enforcement measures, such as: the unauthorized use of protected content is subject to a 3 year imprisonment and a fine of €300 thousand; the failure to pay remuneration to the copyright holder in the context of a use subject to a legal license, e.g. private copying or public lending, is subject to a fine of €300 thousand; the use or dissemination of a computer program manifestly intended to communicate unauthorized works to the public is subject to a three-year imprisonment and a fine of €300 thousand; the violation of TPMs is subject to a six-month imprisonment and a fine of €30 thousand. Other measures include: the closure of establishment that served for commission of offence, and confiscation, destruction and publicity measures. There are also specific sanctions for legal entities, which entail higher fines than for individuals.³³⁹

GERMANY

The German Copyright Act imposes a number of criminal enforcement measures, which can lead to fines and prison terms; the latter can be increased if the offence is deemed to occur on a commercial scale. Offences include the unlawful exploitation of works and the infringement of related rights (subject to 3 or 5 years if on a commercial scale, or fine), and the infringement of TPMs and RMI (subject to 1 or 3 years if on a commercial scale, or fine). Beyond prison terms and fines, enforcement measures include confiscation and publication. Criminal offences can only be prosecuted upon a complaint filed by the aggrieved party, unless the competent authority regards action to be necessary on account of its particular public interest.³⁴⁰

According to the national expert, these provisions are not relevant in practice, as the available private claims are sufficient to address infringement. In particular, it is not necessary to start criminal proceedings to obtain personal information of the infringer (see *infra* at 4.4).³⁴¹

THE NETHERLANDS

Under Dutch law, the general rule is that anyone who intentionally infringes another person's copyright is punishable with imprisonment for not more than six months or with a fine. This requires (criminal) intent and proof of actual copyright infringement by the suspect.³⁴² These sanctions can be substantially elevated (imprisonment for a term of not more than four years or a fine up to €82 thousand) if the crimes are committed by a person who makes it his profession or business to commit

³³⁷ Ibid.

³³⁸ Sec. 27 Computer-Related Crime Act.

³³⁹ Report France. See art. L.335-3 (1) and (2) France IPC.

³⁴⁰ Sects 106 to 111a German Copyright Act.

³⁴¹ Report Netherlands.

³⁴² Art. 31 Dutch Copyright Act. NB that certain acts are subject to higher prison terms and fines. See Art. 31a Dutch Copyright Act, which establishes a lower burden of proof. See Report Netherlands.

the crimes referred to in those provisions.³⁴³ Finally, anyone that offers for distribution, possesses with an intent to use, or in general makes a commercial use of means for the sole intended purpose of facilitating the unauthorized removal or circumvention of TPMs, is punishable with imprisonment for a term of not more than six months or with a fine of the fourth category (max. € 16.750; as of 1 January 2016: €20.5 thousand).³⁴⁴

POLAND

Polish law contains criminal measures in the Copyright Act and Criminal Code, including imprisonment, restriction of liberty, criminal fines, and confiscation of the means used to commit a criminal offence.³⁴⁵ Crimes include e.g. unauthorized use of works, their unauthorized dissemination, the manufacture or distribution of TPM circumventing devices. Prison terms increase if the intention of the infringer is to gain material benefits, and if he makes the offence a regular source of income, or organizes or manages a criminal activity.³⁴⁶

SPAIN

The current version of Article 270 of the Spanish Criminal Code was last amended in 2015. Paragraph (1) provides criminal measures against a person who “with direct or indirect economic profit and in prejudice of a third party, reproduce, plagiarize, distribute, communicate to the public or economically exploits in any manner, all or part of a literary, artistic or scientific work or its transformation, performance or execution fixed in any format or communicated by any means”.³⁴⁷ Furthermore, paragraph (2) introduced a new crime new crime tailored for websites that offer links to infringing contents (on P2P and other platforms) and regardless of whether their activity qualifies as a copyright infringement or not.³⁴⁸

Under the prior wording of Article 270 (mentioning “lucrative intent” instead of direct or indirect economic profit”), Spanish courts interpreted this language restrictively as meaning that criminal copyright sanctions required “commercial intent” and were reserved for the “most serious cases”, thereby avoiding “excessive criminalization” and overlap with civil remedies. With the 2015 amendment the letter of the law became more encompassing. However, the Spanish General Prosecutor promptly issued Circular 8/2015 (21 December 2015) to clarify that the new wording applies to infringers with a “commercial lucrative intent”, thereby excluding most P2P users. Despite this, the Spanish expert notes a tendency since 2015 for courts to increasingly condemn copyright infringement massively conducted online.³⁴⁹

Sanctions for copyright crimes include cumulatively fines and imprisonment, depending on whether the crime in question is regular or aggravated. A regular copyright crime is subject to a fine corresponding to 12 to 24 months and imprisonment of 6 months to 4 years. An aggravated crime exists when the profit obtained has major economic effects, or when the harm caused is particularly serious, or when the infringer belongs to an organization dedicated to commit copyright infringements, or when minors are used to commit these crimes. Such a crime is subject to a fine corresponding to 18 to 36 months and imprisonment of 2 to 6 years. Spanish law also includes the sanction of publication of the ruling at the expense of the infringer.³⁵⁰

³⁴³ Art. 31b Dutch Copyright Act.

³⁴⁴ Art. 32a Dutch Copyright Act.

³⁴⁵ Arts 115-118, 278, and 299 Polish Copyright Act.

³⁴⁶ Ibid.

³⁴⁷ Art 270(1) Spanish Penal Code.

³⁴⁸ See Report Spain, citing Art. 270(2) Spanish Criminal Code (amended in January 2015 by LO 1/2015). This provision is aimed at ISP that, “with the aim of obtaining a direct or indirect economic profit and to the prejudice of third parties, facilitate in an active and non-neutral manner, rather than only doing a merely technical processing, online access to or location of [infringing works or subject matter]..., in particular by providing ordered and classified lists of links to these works and even though these links had been initially provided by the users of their services”.

³⁴⁹ Report Spain.

³⁵⁰ Arts 270, 271, 272(2), and 288 Spanish Penal Code.

SWEDEN

Under Swedish law, copyright infringement is regarded as criminal in nature because criminal sanctions can be imposed, namely fines and imprisonment, confiscation of property, and seizure of property.³⁵¹ Fines and imprisonment (up to 2 years) are only available if a user acts intentionally or with gross negligence. These are available for all categories of protected content with the exception of the reproduction of computer programs (and by extension video games and digital compilations) for personal and non-commercial use, which is exempted from criminal liability on condition that the original copy of the computer program that was reproduced is not being used for commercial purposes or in the public sector. An example of the application of criminal sanctions to online use is the 2016 case of a user been sentenced to a penalty fine and given a suspended sentence for contributory infringement of the communication to the public and reproduction rights by having arranged, provided and administered a file-sharing website, which was hosted on its personal computer.³⁵²

UK

The UK CDPA includes criminal sanctions for a variety of different acts of direct infringement.³⁵³ For the purposes of this report, the most important rule is that a person who infringes copyright in a work by communicating it to the public commits an offence, if that person (1) knows or has reason to believe that s/he is infringing copyright in the work; and (2) s/he either (i) intends to make a gain for him/herself or another person, or (ii) knows or has reason to believe that communicating the work to the public will cause loss to the owner of the copyright, or will expose the owner of the copyright to a risk of loss.³⁵⁴ A person guilty of such an offence is liable: on summary conviction to a fine or imprisonment for a term not exceeding 10 years or both; or on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years or both.³⁵⁵ In addition, search orders may be available.³⁵⁶

- Americas (Brazil and Canada)

In **Brazil**, copyright infringement is considered a crime under the Brazilian Penal Code.³⁵⁷ Crimes include standard copyright infringement (imprisonment up to 1 year *or* fine; dependent on criminal complaint) and different types of aggravated infringement (for profit purposes imprisonment up to 4 years *and* fine; public criminal action, in some instances dependent on representation by rights holder). An important feature is that no crime applies if the act in question is privileged by an exception or limitation, or if the copier makes one single copy of the work/subject matter for private non-commercial use (e.g. downloading and stream-ripping).³⁵⁸

In **Canada**, the Copyright Act criminalizes both copyright infringements and circumventions of TPMs for commercial purposes. Offenders are liable: (1) on conviction on indictment, to a fine of not more than \$1 million or to imprisonment for a term of not more than 5 years or to both; or (2) on summary conviction, to a fine of not more than \$25 thousand or to imprisonment for a term of not more than six months or to both.³⁵⁹

- Asia (Hong Kong, Indonesia, Japan, Thailand)

³⁵¹ Secs 53, 53a and 59(3) Swedish Copyright Act.

³⁵² Svea Court of Appeals 16 March 2016, Case B 1910-15.

³⁵³ Secs 107-110 UK CDPA 1998.

³⁵⁴ Sec. 107(2A) UK CDPA 1998. See also Sec. 107(2B) UK CDPA 1998 for the notions of “gain” and “loss”.

³⁵⁵ Sec. 107(4A) UK CDPA 1998.

³⁵⁶ See Sec. 109 UK CDPA 1998 and Report UK for further detail.

³⁵⁷ Art. 184 Brazil Penal Code.

³⁵⁸ Art. 184(4) Brazil Penal Code.

³⁵⁹ Secs 42(1), 42(2.1), and 42(3.1) Canadian Copyright Act.

HONG KONG

Under the HK Ordinance, a copyright infringer may be liable on conviction on indictment to a fine at level 5 (HK\$ 50 thousand) in respect of each infringing copy and to imprisonment for 4 years. In addition, under the HK Crimes Ordinance, a person who accesses a computer with criminal or dishonest intent may be liable on conviction upon indictment to imprisonment for 5 years.

INDONESIA

Under Indonesian law, online copyright infringement is subject to fines and imprisonment up to a maximum, respectively, of 1 billion rupiah and/or 4 years.³⁶⁰ The law further defines stricter penalties for what it qualifies as “piracy”, i.e. the unauthorized reproduction/duplication or works or its massive distribution for commercial/profit purposes. In this case, the sanctions may amount to a fines and imprisonment up to a maximum, respectively, of 4 billion rupiah (approximately USD 296 thousand) and/or 10 years.³⁶¹

JAPAN

The Japanese Copyright Act provides that an infringement of copyright is punishable by imprisonment with work obligation for up to ten years or by a fine of up to JPY 10 million, or both.³⁶² An illustration of the application of this to online infringement is the 2014 case of the manager of a stream-ripping website that enabled users to download music as MP3 files from a video sharing platform. The manager was arrested on the grounds that he was directly infringing copyright.³⁶³

THAILAND

Under the Copyright Act of Thailand, a criminal lawsuit can be filed against an infringing user within 3 months of the infringement; otherwise the prosecution is barred by prescription. The lawsuit may be filed by the copyright holder or through the public prosecutor. Regular crimes of copyright infringement (i.e. offences against protected music, audio-visual works, books and videogames) are punishable by a fine of 20 thousand Baht up to 200 thousand Baht (approximately USD 600-5.990). The offence is aggravated if committed with a commercial purpose, in which case the infringer is subject to imprisonment for a term from 6 months up to 4 years, or a fine of 100 thousand Baht up to 800 thousand Baht (approximately USD 2.994-23.952), or both imprisonment and fine.³⁶⁴

If a person sells Kodi boxes or similar devices (with pre-installed add-ons linking to unauthorized websites) for profit, a fine between 10 thousand and 100 thousand Baht (approximately USD 300-2.994) can be imposed. Again, the offence is aggravated if committed with a commercial purpose, in which case the infringer is subject to imprisonment for a term from 3 months up to 2 years or a fine of 50 thousand Baht up to 400 thousand Baht (approximately USD 1.497 -11.975), or both imprisonment and fine.

Variation per type of content

As mentioned, national experts were asked to note any differences that may apply in enforcement measures depending on the type of protected content, namely music, audio-visual, books, and video games. As rule, there were no significant differences reported in this respect.

³⁶⁰ Report Indonesia, citing Art. 113(3) Indonesia Copyright Act.

³⁶¹ Report Indonesia, citing Arts 1(28) and 113(3) Indonesia Copyright Act.

³⁶² Art. 119(1) Japanese Copyright Act.

³⁶³ Report Japan.

³⁶⁴ Sec. 69 Thailand Copyright Act.

One exception can be found in Polish law, which includes special criminal offences that only apply to software and works including software, such as video games. One example is the offence of acquiring someone else's computer software without permission and with the purpose of gaining a material benefit, which is subject to an imprisonment term between 3 months and 5 years.³⁶⁵

4.2. Enforcement measures available against intermediaries

This subsection deals with enforcement measures that apply to intermediaries that act in that capacity. Where the activities of intermediaries are qualified in national law as direct infringement of copyright, the measures discussed above at 4.1 apply. Here we discuss the specific civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions available under national law against intermediaries to address online copyright infringement by third party users of their services. To the extent any measures of this type are discussed above under the heading "liability of online intermediaries" (3.3) we will make reference thereto. When addressing this topic, national experts were asked to note any differences that may apply depending on the type of protected content, namely music, audio-visual, books, and video games.

Civil

- EU

Under EU law, as noted, intermediaries that qualify for the safe harbors in the ECD are not liable for damages but only for injunctions – pursuant to Article 8(3) of the InfoSoc Directive – and duties of care, as permitted by the ECD and further established in national law. In all cases, measures must not conflict with the general prohibition against monitoring (under the national equivalent to Article 15 ECD) and must strike a fair balance between competing fundamental rights in line with CJEU case law (see *supra* at 2.2).

FRANCE

Under this heading, the French expert points out two measures that may apply to intermediaries. First, if a computer program is mainly used for unlawfully making available protected content, e.g. P2P software, the President of the High Court of First Instance may, ruling in summary proceedings, order under penalty all necessary measures to protect this right in accordance with the state of the art. Subject to certain conditions, such measures may include the implementation of filtering processes to prevent infringement.³⁶⁶ Second, in presence of copyright infringement, the High Court of First Instance may order any person likely to remedy the situation to implement measures to prevent or to block the infringement acts, including ISPs used for infringement acts.³⁶⁷ Regarding the latter, the French Supreme Court ruled that the French Union of Phonographic Publishing could request that Google be ordered to remove certain suggestions from its "Google Suggest" service, which automatically presents popular searches while the Internet user types his search.³⁶⁸

GERMANY

Under German law, the national expert points to the following remedies available against intermediaries. The first relates to the aforementioned concept of "interferer liability" (*supra* at 3.3) and the availability of injunctions against any person who has willfully made a causal contribution to the direct copyright infringement by a third party (e.g. running an online platform), if that contributor violated a reasonable duty of care to prevent such direct infringements. Typically, the duty in question

³⁶⁵ Report Poland, citing Arts 278(2) and 299 Polish Criminal Code.

³⁶⁶ Art. L.336-1 France IPC.

³⁶⁷ Art. L.336-2 France IPC.

³⁶⁸ Report France, citing Cass. civ. 1, 12 July 2012, 11-20358.

consists of deleting the content of third parties upon notification in the context of a NTD-type procedure. In addition, the “interferer” must take reasonable measures, such as filtering, to prevent further comparable infringements in the future.³⁶⁹ In addition, under a provision on the right to information, German law imposes on the intermediary obligations to inform the copyright holder about the direct infringer.³⁷⁰

THE NETHERLANDS

Dutch law contains several measures potentially applicable to intermediaries, such as NTD, website blocking, and measures for the identification of infringers. Regarding NTD, reference is made to the above description of the voluntary code of conduct adopted by Dutch intermediaries (and developed with the government and interest groups) in order to benefit from safe harbor protection for hosting and caching activities under Article 6:196c of the Civil Code (*supra* at 3.3).

Furthermore, Article 26d of the Dutch Copyright Act allows authors to apply for court injunctions to order an intermediary whose services are used by a third party to infringe copyright, to cease and desist from providing the services that are used for that infringement. On this basis, Dutch courts order the blocking of domain names and IP addresses of infringing websites. There has been discussion in the courts as to what constitutes “effective” blocking of websites, a matter which has yet to be ultimately decided.³⁷¹

Finally, Dutch law allows for injunctions against a third party – such as an intermediary – whose services are used for infringement on a commercial scale to provide information on the infringement.³⁷² Although the intermediary can refuse to provide the information, such refusal can serve as evidence of participation in an infringement of copyright (see *infra* at 4.4, on the issue of disclosure of personal data).

POLAND

Outside the context of the safe harbors and NTD requests, the only measures available against intermediaries under Polish law are general preventive injunctions and damages, although in both cases they are considered by the expert “difficult to implement”. Notably, injunctions against intermediaries as envisaged in Article 8(3) InfoSoc Directive are not available.

SPAIN

Following the ECD, Spanish law allows for injunctions and precautionary measures against intermediaries irrespective of applicable safe harbors. In this context, ISPs may be ordered to suspend the Internet service provided to the infringer, block access to and/or remove infringing content hosted on its server, and publish notices regarding the infringement.³⁷³ Furthermore, blocking injunctions of infringing websites may be directly sought against Internet access providers, rather than suing the individual infringers / website operators, as the law allows that injunctions be sought not only against the infringer but also against any “intermediaries” whose services are being used to infringe copyright, even if these are not themselves infringing copyright.³⁷⁴ In addition, since 2014, ISPs may be ordered to provide information to identify the infringer “in some special cases” in civil

³⁶⁹ Report Germany, citing BGH, 12.7.2012 – I ZR 18/11 paras 29, 32 – *Alone in the dark*, and referring to this model as “notice-and-action”.

³⁷⁰ Sec. 101 German Copyright Act (Right of information).

³⁷¹ Report Netherlands, citing Appellate Court Den Haag 28 January 2014, ECLI:NL:GHDHA:2014:88, Ziggo/Brein, par. 5.24-5.26 (blocking access to the online sharing platform ‘The Pirate Bay’ is ineffective and should therefore be discontinued) and (Supreme Court 13 November 2015, ECLI:NL:HR:2015:3307, Brein/Ziggo, par. 4.4.2 (holding that the Court of Appeals had applied too stringent criteria to test the effectivity of the website blocking order).

³⁷² Art. 28(9) Dutch Copyright Act.

³⁷³ Arts 138-139 TRLPI.

³⁷⁴ Report Spain, citing Art.138 TRLPI.

proceedings, a possibility only previously available in criminal proceedings.³⁷⁵ Finally, the Spanish expert also notes the reluctance of national courts in granting injunctions to prevent future infringements, on the fear that this may translate into an obligation to filter or monitor content contrary to Article 15 ECD and the EU Charter.³⁷⁶

SWEDEN

Differently from Article 8(3) of the InfoSoc Directive, Swedish law only allows for enforcement measures against intermediaries if they are at least secondarily liable for infringement (with the exception of an information injunction). Intermediaries may be subject to general injunctions, including interim injunctions and blocking orders. In this respect, the national expert notes that Swedish courts, which typically relied on stricter secondary liability definitions in the Penal Code, have since 2017 introduced a *civil law definition* of secondary liability. The net result of this shift was to effectively broaden the scope of secondary liability. Apart from this aspect, the same rules apply as for injunctions applicable to primary infringers.³⁷⁷ In addition, intermediaries may be subject to the special information injunction, on the same terms applied to direct infringers (on which, see *supra* at 4.1).³⁷⁸

UK

Section 97A CDPA implements into UK law Article 8(3) of the InfoSoc Directive. According to this, the High Court (in Scotland, the Court of Session) shall have power to grant an injunction against a service provider, where that provider has actual knowledge of another person using their service to infringe copyright. In determining this, the court will consider all relevant circumstances, including whether the provider has received a notice in accordance with the terms of the law (including the type of information provided by the right holder).³⁷⁹

Most of the case law applying this provision concerns blocking injunctions, and identifies four conditions to grant the injunction: (1) the defendants must be service providers; (2) the users and/or the operators of the websites targeted for blocking must infringe the claimant's copyrights; (3) those users or operators must use the defendants' services to do that; and (4) the defendants must have actual knowledge of this fact.³⁸⁰

In addition, intermediaries might also be subject to so-called "Norwich Pharmacal" orders (**NPO**), i.e. a form of disclosure order, made under the equitable jurisdiction of the court, used in cases where the identity of the wrongdoer is unknown but it is possible to identify a third party who has this information. For additional detail, see *infra* at 4.4.

- Americas (Brazil and Canada)

BRAZIL

We make reference to the analysis of Brazilian law above at 3.3. As noted there, the Brazilian Copyright Act does not contain express provisions on Internet intermediaries. In addition, the "Internet Civil Act" (*Marco Civil*), which sets out safe harbors for intermediaries, expressly excludes copyright from its scope of application.³⁸¹ As a result, ISPs may be subject to contributory liability

³⁷⁵ Spain Report, citing Act 21/2014 amending Art. 256 Act 1/2000 on Civil Procedure.

³⁷⁶ Ibid., citing AP Madrid (sec.28) January 14 2014 [Telecinco v. Youtube] Westlaw.ES JUR\2014\36900.

³⁷⁷ Report Sweden, citing Art. 53b Copyright Act and PMÖD, Case PMT 11706-15, delivered on 13 February 2017.

³⁷⁸ Ibid., citing NJA 2012 s.975, Sweden Supreme Court (judgment delivered on 21 December 2012), and Case PMÖA 660-16, Patent and Market Court of Appeal (judgment delivered on 18 November 2016).

³⁷⁹ Report UK, referring also to Regulation 6(1)(c) of the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013).

³⁸⁰ Ibid.

³⁸¹ Arts 19 and 31 Brazil Internet Civil Act. See Report Brazil.

under the Copyright Act and the general rules of civil responsibility in the Civil Code and Consumer Rights Code. Building on these provisions, the Superior Court of Justice has developed a tort law based secondary liability (or “subsidiary responsibility”) regime for hosting providers, which regime is summarized above at 3.3. Failing to meet the conditions set forth in this judge-made doctrine of contributory liability, ISPs are apparently subject to remedies such as injunctions and damages.

CANADA

We make reference to the analysis of Canadian law above at 3.3. As noted there, the Canadian Copyright Act shelters most intermediaries (e.g. ISPs, hosting providers, and search engines) from civil liability for copyright infringement by their users. This is the result of a general provision complemented by specific safe harbors.³⁸² Furthermore, Canadian law includes since the 2015 a “notice-and-notice” regime to discourage online copyright infringement; under this regime, a claimant’s only remedy against an ISP who fails to perform their obligations is statutory damages capped at \$10 thousand.

Canadian law then contains an exception to the safe harbors under the so-called “enabler” liability provision, according to which it is an infringement of copyright to provide a service primarily for the purpose of enabling acts of copyright infringement if an actual infringement of copyright occurs as a result of the use of that service. This provision – yet to be subject to judicial interpretation – could apply to certain intermediaries, such as *The Pirate Bay* or *Popcorn Time*.³⁸³ Canadian law further includes a similar provision that prohibits providing services or manufacturing technology primarily for the purposes of facilitating the circumvention of TPMs.³⁸⁴

Finally, under Canadian law it is possible for right holders to ask a court to identify alleged infringers through an equitable bill of discovery, also known as a Norwich order (similar to the UK NPO mentioned above). If the request is successful, the court can compel a non-party intermediary to share the subscriber’s details (see *infra* at 4.4).

- Asia (Hong Kong, Indonesia, Japan, Thailand)

HONG KONG

Depending on the online intermediaries’ degree of involvement and whether they take steps to ensure the removal of infringing content, they may be liable for infringement by authorisation or contributory infringement. If so, they are subject to similar civil remedies as direct infringers (*supra* at 4.1), namely injunctions and takedown orders, damages, and account of profits. Injunctions against the online intermediaries may include: takedown orders against forums; website blocking orders against ISPs; and de-indexing orders against indexing and bookmarking sites, including search engines. It is noteworthy that the last two types of injunctions have yet to be tested before the Hong Kong Courts, although the national expert expects courts to largely follow the approach in England under its wide powers to grant injunctive relief.³⁸⁵

INDONESIA

Under Indonesian law, as noted, the liability of intermediaries results from a duty of care principle in Article 1367 Civil Code regarding accountability for damages caused by persons and properties under their responsibility or supervision. The national expert notes that neither the ITE Law nor the Copyright Act determines enforcement measures available against intermediaries in this respect, but

³⁸² Secs 2.4(1)(b), 31.1(1)-(2),(4), 41.27(1) Canadian Copyright Act.

³⁸³ Report Canada, citing Sec. 27(2.3) Canadian Copyright Act and mentioning the case of the lawsuit filed by Music Canada against isoHunt Web Technologies Inc. and Gary Fung (isoHunt offered a bittorrent search service). B.C. Sup. Ct. File No. S086309, settled on consent July 13, 2016.

³⁸⁴ Sec. 41(1)(b)-(c) Canadian Copyright Act.

³⁸⁵ Report Hong Kong.

the breadth of the general duty of care likely entails that platforms are liable for the copyright infringement actions of their users. Presumably, they would avoid liability if they can prove to be “unable to prevent the act, for which they would be liable” (Article 1367 Civil Code, *in fine*). If liable, an intermediary is subject to the same civil remedies as direct infringers (*supra* at 4.1).³⁸⁶

JAPAN

Japanese law does not contain any statutory provision or judicial doctrine that allows injunctions against intermediaries in terms similar to Article 8(3) InfoSoc Directive or “interferer” liability in Japan. Despite that, the national expert notes that in the aforementioned *TV Break Case*, where an injunction was issued against a video-sharing platform on the grounds of direct infringement, primary liability was imposed on the platform because it incited its users to upload content with a commercial intent, and neglected any measures to prevent infringement.³⁸⁷ Also, under the ISP Liability Limitation Act, an injunction may be obtained for ISPs to disclose information of infringing users in their possession.³⁸⁸

Finally, under the general rules of the Civil Code, an intermediary can be considered jointly and severally liable to compensate for damages as a joint tortfeasor if it has incited or was an accessory to copyright infringement.³⁸⁹

THAILAND

Under the law of Thailand, namely the wrongful acts of the Civil and Commercial Code, intermediaries may be subject to remedies of damages and injunctions if they are negligent and cause damages to right holders.

Administrative

To the extent intermediaries qualify as users due to the nature of their activities, they will be subject to the administrative measures mentioned above at 4.1. The only national laws that contain administrative measures specifically targeting (online) intermediaries are those of Spain, the UK, Indonesia, and Thailand.

SPAIN

As noted above (at 4.1) Spanish law has since 2011 (with an amendment and enlargement in 2014) an injunction procedure by the Intellectual Property Commission or “CPI” (sec. 2) against infringements done for commercial purposes by ISPs. The CPI (sec. 2) is entitled to issue injunctions against two types of infringement:

- Against ISPs that significantly infringe copyright, an assessment is made prior to starting proceedings based on factors such as the Spanish audience of the site, the amount of infringing works it provides access to, and its business model.
- Against ISPs that facilitate the location of infringing content by providing ordered and classified lists of links – regardless of whether such links are initially provided by users of the service – when the ISP acts in an “active and non-neutral” manner. (Naturally, this design is influenced by CJEU case law on the ECD safe harbors).³⁹⁰

³⁸⁶ Report Indonesia.

³⁸⁷ Report Japan, citing IP High Court, 8 September 2010, 2115 Hanrei Jihō 102 [*TV Break Case*]. A translation is available at <<http://www.ip.courts.go.jp/hanrei/pdf/20111115132355.pdf>>.

³⁸⁸ Ibid., citing Art. 4(1) ISP Liability Limitation Act.

³⁸⁹ Ibid., citing Art. 719(2) Japanese Civil Code.

³⁹⁰ Report Spain.

Under this regime, the failure by the ISP to withdraw content or cease infringement entitles the CPI (sec. 2) to order: the ISP to block access to or remove infringing contents; the access provider to stop its service to the infringing site; the cancellation of “.es” domain names; and the suspension of third party advertising on the infringing site. Also, infringers or ISPs that do not comply with the CPI’s orders are subject to fines up to €600 thousand. An important feature is that rulings by the CPI (sec. 2) are subject to prior judicial approval by an administrative court.³⁹¹

The national expert notes that injunctions so validated tend to be confirmed on appeal. Existing data is not conclusive. On the one hand, they are slow (average resolution time of 480 days) and very few injunctions have been adopted since 2011. On the other hand, there is data suggesting that around 300 infringing websites have ceased their infringing activities as a result of such measures.³⁹²

UK

Reference is made to the administrative measures mentioned above (at 4.1), namely the Voluntary Copyright Alert Programme (VCAP). This system is relevant to intermediaries to the extent that their services are enlisted to send notices to end-users.

INDONESIA

As noted, the 2015 Joint Regulation of the Minister of Law and Human Rights and the Minister of Communication and Information, based on Article 55 of the Copyright Act, deals *inter alia* with the responsibility of intermediaries (see *supra* at 4.1 for a description of this instrument). According to the expert, intermediaries are given some discretion on how to deal with infringing content or activities carried out by third parties using their services. In practice, if a third party is infringing copyright in this way, the intermediary will first send the user a warning letter to cease the infringement and/or terminate its contract. In the latter case, the termination will entail the blocking or deletion of the allegedly infringing content. In addition, the expert notes the possibility that the user’s Internet access is suspended pending the finalization of the process for producing evidence of the infringement by the Ministry of Communication and Information (see the procedure described *supra* at 4.1).

THAILAND

Under the law of Thailand, certain administrative enforcement measures are available against intermediaries, namely resulting from actions of government officers without a requirement that the injured party initiates civil or criminal procedures.

In particular, two measures are available that would meet such a definition, according to the national expert. First, under Article 32(3) of the Copyright Act, it is possible for a court order to be issued against a service provider to remove infringing content from its system. The competent court is Central Intellectual Property and International Trade Court. Second, the Computer-Related Crime Act provides for an administrative enforcement measure aimed at stopping the dissemination of information or deleting of data from systems, where that information/data qualifies as criminal copyright infringement.³⁹³ We make reference to 4.1 above, where this measure is described.

The measures have different consequences for service providers. The provider that disregards the Court order issued under the Copyright Act faces no penalty; however, he is then subject to a *civil* lawsuit as mentioned above in this subsection. Differently, failure to comply with the measure ordered under the Computer-Related Crime Act subjects the provider to a general fine up to 200 thousand

³⁹¹ Ibid.

³⁹² Ibid, citing several sources on the activity of the CPI (sec. 2).

³⁹³ Sec. 20 Thailand Computer-Related Crime Act. NB: the petition can be electronic.

Baht and further daily fines not exceeding 5 thousand/day until the relevant corrective action is taken.³⁹⁴

Criminal

Most national laws do not contain criminal measures specifically targeting (online) intermediaries. To the extent intermediaries commit, or are involved in (by assisting or inducing others) any of the crimes of copyright infringement defined in national law, they are subject to the criminal measures mentioned above at 4.1. Apart from that, it is worth mentioning certain aspects in the laws of Spain, Sweden, the UK, and Japan.

SPAIN

In 2015, Spanish law introduced a new crime tailored for websites that offer links to infringing contents (e.g. on P2P and other platforms), regardless of whether their activities are themselves infringing.³⁹⁵ However, the provision does not apply to ISPs that provide “merely technical intermediary services, such as neutral search engines” or to ISPs that only “occasionally link to third party infringing contents”.³⁹⁶

SWEDEN

Under Swedish law, intermediaries may be subject to criminal measures, such as fines and imprisonment, confiscation and seizure of property, and the regime on responsibility for Electronic Bulletin Boards.

Regarding fines and imprisonment, the general provision on direct criminal copyright infringement (penalty fine or imprisonment for up to two years) applies also to secondary liability by virtue of reference in the Swedish Penal Code. The specific penalty prescribed depends on the level of intention and/or negligence attributable to the intermediary qualified as a contributor.³⁹⁷ On confiscation and of seizure of property, the same rules apply as for direct infringement (see *supra* at 4.1.).

Finally, the Act on Responsibility for Electronic Bulletin Boards provides that the operator or provider of such services may be subject to a financial penalty or imprisonment for up to six months, or for up to two years for a serious crime, if he intentionally or with gross negligence fails to remove a message whose posting is an obvious copyright infringement. However, if the provider or operator can also be held liable under the Copyright Act, the provision does not apply.³⁹⁸

UK

Under UK law, as with most national laws, intermediaries will be held criminally liable in the same way as other infringers or as secondarily liable for a primary offender’s acts.³⁹⁹ It is in addition possible for intermediaries to be held criminally liable if they have manufactured articles specifically designed or adapted to make copies of a particular work, or have such articles in their possession, knowing or having reasons to believe that they are to be used to make infringing copies for sale, hire or use in the course of a business. In that case, the intermediary can be held liable on summary

³⁹⁴ Report Thailand.

³⁹⁵ Art. 270(2) Spain Penal Code, introduced by the LO 1/2015.

³⁹⁶ Report Spain, citing the Preamble of LO 1/2015.

³⁹⁷ Report Sweden, citing Art. 53(1) Swedish Copyright Act and Ch. 23 Sec. 4(1) Swedish Penal Code.

³⁹⁸ *Ibid.*, citing Art. 7(1) Act on Responsibility for Electronic Bulletin Boards.

³⁹⁹ Report UK, citing Sec. 107(2A) UK CDPA and Sec. 8 of the Accessories and Abettors Act 1861. The latter that criminal sanctions may be imposed upon those who aid, abet, counsel or procure the commission of an offence.

conviction to imprisonment (maximum 3 months), or will be imposed a fine (maximum level 5), or both.⁴⁰⁰

JAPAN

Other than the measures applicable to accessories to a crime in the Japanese Penal Code (Article 62(2)), the national expert makes reference to a court case concerning the “Winny” file sharing software. In this case, after the Kyoto District court convicted a person who released the software of a crime of inducing third party copyright infringement, both the Osaka High Court and later the Supreme Court denied the crime on the ground that the accused lacked intent to be an accessory to the crime of copyright infringement.⁴⁰¹

Variation per type of content

As mentioned, national experts were asked to note any differences that may apply in enforcement measures depending on the type of protected content, namely music, audio-visual, books, and video games. As rule, no significant differences were reported.

4.3. Differences in public and private enforcement per type of protected content

On this topic, experts were asked whether, to the best of their knowledge, there are significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games). In this context, the notion of enforcement “practices” refers to the reality of enforcement in the field, including agreements between stakeholders for the enforcement of copyright online (e.g. codes of conduct for NTD directed to ISPs that provide a public telecommunications service).

For the majority of countries no significant differences were noted. This is the case of France, Germany, The Netherlands, Sweden, Hong Kong, Indonesia, Japan, Thailand, and Canada. For the remaining countries in the study, some aspects are worth mentioning. Finally, although no differences were noted for the UK, the existence of two Codes of Conduct in this jurisdiction should be pointed out.

In **Poland**, as noted, there are legal differences in the treatment of video games as software (meaning that they do not benefit from the private copying exception) and special criminal offences that apply only to software and works including software, such as video games.⁴⁰² These, however, do not translate into significant differences in enforcement practices, according to the expert.⁴⁰³

In **Spain**, in addition to the enforcement measures described above, it is noted that most CMOs (upon request of their members) notify ISPs about infringing content available on their websites and threaten with judicial action unless that content is blocked or removed/delisted. According to CMOs, ISPs usually tend to comply with these notifications.⁴⁰⁴

In **Sweden**, injunctions against ISP require at least a showing of contributory infringement, with the exception for information injunctions. This fact, combined with the absence of more specific rules

⁴⁰⁰ Ibid., citing Secs 107(2) and (5) UK CDPA.

⁴⁰¹ Report Japan, citing Supreme Court, December 19, 2011, 65-9 Keishū 1380 [Winny Case]. The translation is available at <http://www.courts.go.jp/app/hanrei_en/detail?id=1131>.

⁴⁰² *Supra* at 3.1 (Downloading) and 4.1 (variation per type of content)

⁴⁰³ Report Poland.

⁴⁰⁴ Report Spain.

beyond ECD-type safe harbors, creates a framework that arguably disincentives ISPs from developing common codes of conduct for NTD procedures.⁴⁰⁵

In **Brazil**, the expert notes incongruity between statutory law, court decisions and private practice. On the one hand, the Copyright Act points to the need of a judicial decision to oblige ISPs to remove illegal content. The Internet Civil Act does not apply to copyright, and the Civil and Consumer Rights Codes only provide general guidance on the issue. Against this backdrop, the Superior Court of Justice has developed a tort law based secondary liability (or “subsidiary responsibility”) regime for hosting providers according to which the non-compliance with an out-of-court notification by the right holder suffices to establish copyright infringement by that intermediary (*supra* at 3.3 and 4.2). In other words, a private notice is sufficient to give rise to liability for the ISP. In addition, the expert notes that there are different types of copyright crimes, some of which may require an initial complaint by the injured right holder or even their intervention in the process.

Finally, in the UK, as noted, there are significant differences as regards public and private enforcement. However, it is worth pointing out the existence of two Codes of Conduct. The first is the Voluntary Copyright Alert Programme (VCAP), which forms part of the industry-led scheme Creative Content UK, and is discussed above (in the context of *administrative enforcement measures* at 4.1 and 4.2). The second is the Voluntary Code of Practice on Search and Copyright agreed in early 2017 by leading search engines, entertainment trade bodies, and music industry body BPI, in a deal brokered by the UK Intellectual Property Office. Under the Code, search engines commit to the removal of links to websites that have been repeatedly served with copyright infringement notices from the first page of their search results, with the aim of preventing UK internet users from downloading and streaming protected content illegally. These commitments include specific targets for reducing the visibility of infringing content in search results.⁴⁰⁶

4.4. Disclosure of personal data in the context of enforcement

This subsection refers to a specification of enforcement measures available against intermediaries, described *supra* at 4.2. In particular, experts were asked whether online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to right holders. In case they do, what conditions must be met for that obligation to arise? For example, is such disclosure only possible after a judicial court order, administrative proceedings, or simply at the request of right holders? Finally, experts were asked what type of personal data is typically requested in this context.

- EU

As noted (*supra* at 2.2), the Enforcement Directive provides in Article 8 for a right to information. It was also noted that the CJEU has interpreted Article 8 of the InfoSoc Directive in *Promusicae* as not imposing nor preventing member states from mandating ISPs to disclose personal data of their subscribers in the context of copyright infringement proceedings.⁴⁰⁷

FRANCE

Under French law, intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to right holders, pursuant to a judicial order. ISPs have an obligation to hold and conserve data for a period of 1 year that will lead to the identification of anyone who has

⁴⁰⁵ Report Sweden, noting however that the judicial broadening of the definition of secondary liability may counteract this.

⁴⁰⁶ Report UK (answer to Question), citing <https://www.gov.uk/government/news/search-engines-and-creative-industries-sign-anti-piracy-agreement>. See also Gov.UK, *FOI release: Search engines and creative industries anti-piracy agreement*, <https://www.gov.uk/government/publications/search-engines-and-creative-industries-anti-piracy-agreement>.

⁴⁰⁷ CJEU, *Promusicae*. See also Bechtold, 2016, p. 485.

contributed to the creation of content.⁴⁰⁸ The data in question is specified by law and includes: the types of protocols used to connect to the service and to transfer the contents; the contractual information of the subscriber; the username at the time of account creation, as well as the personal information provided by the user in this context.⁴⁰⁹ Judicial authorities may order the disclosure of this information at the request of the victims of the infringement. Where the infringing user has provided incorrect information to the ISP, the plaintiffs may still judicially demand the ISP to provide additional information based on the IP addresses in question.⁴¹⁰

GERMANY

German law contains an obligation to disclose personal data of individuals to injured parties in copyright infringing activities.⁴¹¹ In order to obtain information about the direct infringer from an intermediary, two conditions must be met: (1) a manifest infringement has to be established, e.g. by identifying an IP address uses P2P file-sharing; and (2) a court order must be obtained.⁴¹² The type of personal data requested is specified by law and consists of the name and physical address of the infringer.⁴¹³

NETHERLANDS

The Dutch implementation of Article 8(1) of the Enforcement Directive allows judicial injunctions against intermediaries for the disclosure of personal data of individuals involved in copyright infringing activities.⁴¹⁴ Depending on the case, what is typically requested are IP addresses used for infringing copyright, account information (names and email addresses used), so-called NAW data of subscribers (name, address, place of residence) and payment details.

In addition, the Dutch Supreme Court has held that online intermediaries may also be obliged to disclose personal data of individuals involved in copyright infringing activities to right holders on the basis of a general duty of care resulting from Article 6:162 of the Dutch Civil Code.⁴¹⁵ On the basis of this general duty of care, intermediaries may be compelled to make their own independent assessment and hand over personal data to right holders without a court order being present. If intermediaries fail to disclose personal data they may be acting unlawfully for not complying with the duty of care imposed on them.⁴¹⁶

POLAND

Polish law provides no legal basis for an obligation to disclose personal data of individuals involved in copyright infringing activities, such as IP addresses and other identifying data. However, right holders may obtain such information in three ways. First, they can file an information claim under Article 80 of the Copyright Act when it is probable that an infringement has been committed. Second, they may notify a law enforcement agency of copyright infringements in order to institute criminal proceedings, which are subject to the probability that a criminal offence was committed by a platform or user. Right holders may then join the proceedings as an injured party. Public enforcement agencies may require providers to identify users and, as parties to criminal proceedings, right holders may

⁴⁰⁸ Art. 6(2) of the Act on Confidence in the Digital Economy (Act No. 2004-575 of 21 June 2004).

⁴⁰⁹ Art. 1 Decree of 25 February 2011 on the conservation and communication of data allowing the identification of any person who contributed to the creation of content published online.

⁴¹⁰ Report France.

⁴¹¹ Sec. 101(2) No. 3 (3) and (9) German Copyright Act.

⁴¹² Sec. 101(9) German Copyright Act.

⁴¹³ Sec. 101(3) No. 1 German Copyright Act.

⁴¹⁴ Art. 28(9) Dutch Copyright Act.

⁴¹⁵ Dutch Supreme Court 25 November 2005, ECLI:NL:HR:2005:AU4019, *Lycos/Pessers*. See Report Netherlands, specifying the conditions developed by the Court.

⁴¹⁶ Report Netherlands.

receive this information. The third option is to file a request to the General Inspector of Data Protection (an administrative measure).⁴¹⁷

SPAIN

Before 2014, Spanish law only allowed disclosure of personal data of infringing users in the context of criminal proceedings.⁴¹⁸ This rule posed obstacles to enforcement efforts, but its legality was confirmed by the CJEU in *Promusicae*. To overcome this restriction, a 2014 amendment introduced language to the effect that right holders may, “in some special cases”, obtain, prior to starting a *civil* lawsuit, some personal data from alleged infringers or operators of websites facilitating infringement (e.g. by means of links to infringing P2P files). This judicial order (an injunction or precautionary measure) may be directed at an ISP or a third party that provides means of payment or advertising to the allegedly infringing pages. The type of personal data that is typically requested is the name, DNI and personal address of the user/infringer.⁴¹⁹

SWEDEN

Swedish law contains an obligation to disclose personal data of individuals to injured parties in copyright infringing activities.⁴²⁰ This “information injunction” implements and goes beyond Article 8 of the Enforcement Directive. Its purpose is not only to allow a claimant to receive further information during an ongoing case, but also to allow a claimant to apply for such an injunction when there is no infringement case pending before the court.⁴²¹ An obligation to provide information can only arise after a judicial court order.⁴²² An applicant may request any information necessary. Typically names and home addresses are requested.

UK

As noted (*supra* at 4.2), intermediaries may be subject to so-called *Norwich Pharmacal* orders (**NPO**). This is a form of disclosure order, made under the equitable jurisdiction of the court, used in cases where the identity of the wrongdoer is unknown but it is possible to identify a third party who has this information. As an illustration, an NPO was issued in a 2012 copyright case against an ISP for the purpose of disclosure of identifying information on its infringing subscribers, in the context of an unauthorised P2P file-sharing of pornographic films. Following the lead of the CJEU in *Promusicae*, the High Court, after carrying out a balancing test between competing rights at stake (namely copyright vs the rights to privacy and data protection), opted for granting the order but objected to the draft letter to be sent to end users as proposed by right holders. Instead, it endorsed a case-by-case approach and the selection of test cases. The end result was to limit the order to only two of the claimants.⁴²³

- Americas (Brazil and Canada)

BRAZIL

In Brazil, there is no legal obligation to disclose personal data of individuals in copyright infringing activities, as the Internet Civil Act does not apply to copyright. Nevertheless, copyright holders may request and obtain personal data in infringement proceedings by filing a claim for copyright infringement under Articles 102 and 104 of the Copyright Act, and referring to the general obligation in Article 10 of the Internet Civil Act for ISPs to retain personal data. The latter provision obliges

⁴¹⁷ Report Poland, noting the inconsistency of court practices regarding information claims.

⁴¹⁸ Report Spain, citing Art. 12 LSSICE.

⁴¹⁹ Ibid.

⁴²⁰ Sec. 53c-h Swedish Copyright Act.

⁴²¹ Sec. 53e § 1 Swedish Copyright Act.

⁴²² Report Sweden, citing Proposition 2008/09:67, p. 145.

⁴²³ Report UK, citing *Golden Eye & Ors v Telefonica UK* [2012] EWHC 723 (Ch).

ISPs to retain registration data, which includes the affiliation, address and personal qualification, i.e. name, marital status and profession of the user.⁴²⁴

Using this strategy, copyright holders can obtain the personal data of infringers through a court order if they meet the requirements for an infringement claim under the Copyright Act. The court may then order ISPs to provide them with the necessary information to pursue the infringement claim. According to Article 23 of the Internet Civil Act, the data in question must be provided in a justified manner and the confidentiality of the information must be guaranteed in order to preserve the intimacy, privacy, honour and image of the user.

CANADA

As discussed above (at 4.2), Canadian law allows right holders to ask a court to identify alleged infringers through an equitable bill of discovery, also known as a Norwich order (similar to the UK NPO). The legal basis for this court order is Section 7(3) of the Personal Information Protection and Electronic Documents (PIPEDA); without a court order such a disclosure would contravene the PIPEDA. For this order to be granted, the applicant must demonstrate: (1) a valid, bona fide, or reasonable claim; (2) that the intermediary is somehow involved in the acts complained of; (3) that the intermediary is the only practicable source of the information; and (4) that the interests of justice favor the obtaining of disclosure from the intermediary. If the request is successful, the court can compel a non-party intermediary to share the subscriber's details. Right holders typically request the disclosure of subscriber information, i.e. names and addresses, which data allows them to pursue litigation against infringers.⁴²⁵

- Asia (Hong Kong, Indonesia, Japan, Thailand)

HONG KONG

The law of Hong Kong, similarly to the laws of the UK and Canada, allows for a variant of the NPO or Norwich order. In particular, a Norwich Pharmacal application can be filed to compel the disclosure of personal data of an alleged infringer by an online intermediary. The conditions for a successful application are as follows: (1) serious tortious or wrongful activities have been committed; (2) the alleged wrongdoer is a person whom the applicant bona fide believes to be infringing his rights in the sense that he can reasonably be assumed to be the wrongdoer vis-à-vis the applicant; (3) the innocent party, against whom discovery is sought, has been caught up or has become involved in such activities, thus facilitating the perpetration or continuation of the same; and (4) the disclosure must be necessary, proportionate and justified. Typically, the IP address, name and contact details of the user are requested.⁴²⁶

INDONESIA

Although the national expert states such an obligation would derive from the TRIPS Agreement to which Indonesia is a member, national law does not include any legal provision in this respect, nor is there case law to report. It is assumed that the data to be disclosed in such a context would be limited to that relevant for the investigation of copyright infringement (such as the alleged infringer's name, address, profession), at the request of the copyright holder and pursuant to a judicial court order.⁴²⁷

JAPAN

⁴²⁴ Art. 11(2) Decree No. 8.771/2016 Brazil Internet Civil Act.

⁴²⁵ Report Canada, identifying also case law on Norwich orders (Question 12-b).

⁴²⁶ Report Hong Kong, citing in *Cinepoly Records Co Ltd v Hong Kong Broadband Network Ltd* [2006] 1 HKC 433, a case where music producers demanded ISPs to disclose the names, addresses and ID card numbers of persons who allegedly uploaded infringing files through the P2P file sharing programme WinMX.

⁴²⁷ Report Indonesia.

Under Japanese law, a person claiming that his rights have been infringed may demand an ISP (e.g. access and hosting providers⁴²⁸) for disclosure of information in its possession that allows the identification of the infringer, such as the name, address and IP address. This order is subject to the following requirements: (1) evidence that the claimant's rights are infringed by the distribution of the information; (2) the information identifying the infringer is necessary in order for the claimant to exercise his exclusive rights to claim damages; and (3) the claimant has a justified ground to ask for the disclosure of the identifying information.⁴²⁹

THAILAND

According to Section 36 of the Constitution of Thailand, an intermediary can be required to disclose personal data of an alleged infringer based on a court order or a subpoena. No further details were provided by the national expert.

4.5. Entitlement to apply for enforcement measures

This subsection deals with the question of who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law.

- EU

As noted (*supra* at 2.2), the Enforcement Directive contains rules on standing to sue. According to these, the persons entitled to seek **civil enforcement measures** are the right holders, authorized users (e.g. licensees), authorized CMOs, and authorized professional defense bodies.⁴³⁰ The directive further establishes a presumption of authorship and ownership of copyright in favor of authors and related right holders if their name appears on the work or other subject matter “in the usual manner”.⁴³¹ National laws of member states are for the most part consistent with the directive as regards civil enforcement measures, but as the directive leaves some margin of discretion, certain nuances are worth mentioning.

All national laws allow **exclusive licensees** to apply for civil measures, but not **non-exclusive licensees**. In some countries, non-exclusive licensees are explicitly not entitled to apply for civil measures (Germany, Poland and Spain), whereas in others their entitlement is subject to conditions. For instance, in the **Netherlands**, licensees can only apply for such measures provided they have obtained the right to do so from the author or his successor in title (the same requirement applies to CMOs or public defense bodies like *Stichting BREIN*).⁴³² In **Sweden**, entitlement to sue varies according to the specific measure, but exclusive and non-exclusive licensees are usually entitled to apply for injunctions, on the grounds that they may be “affected by an infringement and their need for information to take measures against infringement is as strong as a rightholder’s”.⁴³³ In the **UK**, a non-exclusive licensee may bring an action for infringement of copyright if the infringing act was directly connected to a prior licensed act, the license is in writing and signed by or on behalf of the copyright owner, and the license expressly grants the right of action.⁴³⁴

The laws of four countries – Poland, Spain, Sweden and the UK – do not contain specific provisions allowing professional defense bodies to apply for enforcement measures against copyright

⁴²⁸ Japanese Supreme Court, 8 April 2010, 64-3 Minshū 676 [*Relay Provider Case*].

⁴²⁹ Report Japan, citing Art. 4(1) Japan ISP Liability Limitation Act.

⁴³⁰ Art. 4 Enforcement Directive.

⁴³¹ Art. 5 Enforcement Directive. This provision therefore goes beyond the international standard set in Art. 15 BC, incorporated in TRIPS.

⁴³² Report Netherlands.

⁴³³ Report Sweden, citing Proposition 2008/09:67, p. 129.

⁴³⁴ Report UK, citing Sec. 101A CDPA.

infringement.⁴³⁵ Furthermore, in the UK, it is unclear whether parties other than the right holders may apply for an injunction against service providers under Section 97A CDPA, and the requirements for application of an NPO suggest that the applicant must be a copyright holder.⁴³⁶

As regards **criminal enforcement measures**, not all reports provide detailed information. In **France**, it is merely stated that copyright holders and the police authorities may apply for measures.⁴³⁷ In the **Netherlands**, while copyright holders may report the crime to the police, only the public prosecutor is entitled to start a criminal prosecution.⁴³⁸ In **Poland**, it is noted that some criminal proceedings can be started ex officio.⁴³⁹ In **Spain**, copyright crimes are prosecuted ex officio by the General Prosecutor upon denouncement or report of an infringing activity. Private parties may (but are not required to) join the action as “private accusers”.⁴⁴⁰ In **Sweden**, it is generally the prosecutor who is entitled to apply for enforcement measures. Copyright infringement is categorized as a “public prosecution” crime, meaning that initiation of proceedings by the public prosecutor requires the filing of a complaint by the aggrieved party or that the prosecution is called for in the public interest.⁴⁴¹ Only if the prosecutor elects not to initiate proceedings does private prosecution become available.⁴⁴²

- Americas (Brazil and Canada)

Under **Brazilian law**, copyright holders, assignees and licensees are entitled to apply for *civil* enforcement measures. CMOs can do so as well if the infringement falls within their representation powers. Regarding *criminal* enforcement measures, entitlement to apply for measures depends on the type of criminal offence as regulated by the Criminal Procedural Code. The right holder is entitled to apply for these measures in cases of private criminal actions (e.g. standard copyright infringement) or public criminal actions conditioned to representation (e.g. unauthorized making available to the public of works with a for-profit purpose). The Public Prosecutor is entitled to take action in unconditional public criminal actions (e.g. unauthorized commercial distribution of phonograms).⁴⁴³

Under **Canadian law**, the copyright owner and any person deriving any right, title or interest by assignment from the owner are entitled to apply for enforcement measures. This entitlement applies to exclusive licensees but not to non-exclusive licensees and sole licensees.⁴⁴⁴ Copyright collectives have standing to enforce payment of royalties under an approved tariff or agreement, and may exercise such rights regardless of the mechanism by which they are authorized to act (e.g. assignment, license, appointment as agent or otherwise).⁴⁴⁵

- Asia (Hong Kong, Indonesia, Japan, Thailand)

HONG KONG

Hong Kong law allows the copyright holder and the assignee to apply for *civil* enforcement measures.⁴⁴⁶ However, an *equitable* assignee must join the copyright holder before final relief can be obtained.⁴⁴⁷ Also, an exclusive licensee is entitled to apply for enforcement measures after joinder

⁴³⁵ See Reports Poland, Spain, Sweden, and UK.

⁴³⁶ Report UK.

⁴³⁷ Report France.

⁴³⁸ Report Netherlands, citing Art. 161 Dutch Code of Criminal Procedure and noting that investigations are carried out by a specific body (the Piracy Investigations Team of the Fiscal Information and Investigation Service), as well as that copyright infringement is not “high on its priority list”.

⁴³⁹ Report Poland.

⁴⁴⁰ Report Spain.

⁴⁴¹ Report Sweden, citing Sec. 59 para 1 Swedish Copyright Act

⁴⁴² Ibid., citing Ch. 20, Sec. 8, para. 1 of the Swedish Penal Code.

⁴⁴³ Report Brazil.

⁴⁴⁴ Report Canada, citing Sec. 41.23(1) Canadian Copyright Act.

⁴⁴⁵ Ibid., citing Sec. 34(4)(c) of the Copyright Act.

⁴⁴⁶ Ibid., citing Secs 103(1) & 112(1) HK Ordinance.

⁴⁴⁷ Report Hong Kong, citing *Takmay Industrial Co Ltd v Wah Sang Industrial Co* [1977-79] HKC 115.

with the copyright holder.⁴⁴⁸ Hong Kong law does not provide for criminal offenses for copyright infringement that are “private crimes” or “complaint-based”. Criminal proceedings are usually formally instituted by the Prosecutions Division of the HKSAR Department of Justice. The investigation and arrest stage is usually carried out by the Hong Kong Customs and Excise Department.

INDONESIA

Under Indonesian law, the copyright holder and/or exclusive licensee are entitled to apply for civil, administrative or criminal measures. In addition, CMOs can apply for administrative and criminal enforcement measures. Administrative measures under the Joint Regulation (see *supra* 4.1 and 4.2) can only be pursued if there is first a complaint by the right holder, licensee, or CMO. Finally, criminal copyright infringement in Indonesia is a complaint-based system.⁴⁴⁹

JAPAN

Under Japanese law, it is clear that the copyright holder may apply for civil and criminal enforcement measures in case of copyright infringement.⁴⁵⁰ The national expert further noted that there is strong support for the possibility of the exclusive licensee being entitled to apply for certain civil measures subject to certain conditions, namely injunctions and damages.⁴⁵¹ Furthermore, the Japanese Supreme Court has clarified that the exclusive licensee may also file criminal complaints for copyright infringement.⁴⁵²

THAILAND

Copyright holders and authorized persons (such as licensees and CMOs) are entitled to apply for *civil* enforcement measures.⁴⁵³ *Criminal* enforcement proceedings can be initiated by the damaged person or the public prosecutor.⁴⁵⁴ As noted above (at 4.1 and 4.2), the law of Thailand contains two main *administrative* measures for copyright enforcement. The entitlement to apply for the order for refrain or removal of infringement from a computer system under the Copyright Act lies with the copyright holders and authorized persons. Regarding the order for removal or suppression of dissemination of a copyright infringement from a computer system under Section 20 of the Computer-Related Crime Act, the entitlement to apply for such measures lies with the competent officer, subject to approval from the Ministry.⁴⁵⁵

4.6. Most used and effective enforcement measures

On this topic, experts were asked, to the best of their knowledge, to identify the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in their country. They were asked to indicate whether the measures refer to public or private enforcement,⁴⁵⁶ whether any of the measures was enacted or became more relevant in the

⁴⁴⁸ Ibid., citing Sec. 113 HK Ordinance.

⁴⁴⁹ Report Indonesia, citing Art. 120 Indonesia Copyright Act regarding criminal provisions.

⁴⁵⁰ Report Japan, citing Arts 112(1) and 123(1) Japan Copyright Act.

⁴⁵¹ Report Japan, citing: Tokyo District Court, 31 January 2002, 1818 Hanrei Jihō 165 [*Tonttu doll* Case]; Tokyo District Court, 28 September 2016, Case No.482 (wa) of 2015 [*Smartphone cover* Case]; and Tokyo District Court, 15 April 2015, Case No.24391 (wa) of 2014 [*Amana images* Case].

⁴⁵² Supreme Court, 4 April 1995, 49(4) Keishū 563 (Pirate Video).

⁴⁵³ Report Thailand, citing Sec. 55 Thailand Civil Procedure Code and noting that an “authorized person” is any person that can prove with evidentiary documents that he is authorized by the copyright owner.

⁴⁵⁴ Ibid., citing Sec. 28 of the Penal Code.

⁴⁵⁵ Ibid.

⁴⁵⁶ In this context, “public enforcement” refers to the use of public agents, agencies, bodies or authorities to detect and to sanction copyright infringers, whereas “private enforcement” refers to the threat of litigation by private parties, namely rights holders or their representatives.

practice of enforcement over the last three years, and whether they could provide examples of the application of these measures in high profile cases over that period.

In the analysis that follows, the absence of a specific reference to that effect means that the measures in question were not introduced in the last 3 years and that the national expert did not report any high profile cases.

- EU

FRANCE

In France, with respect to public enforcement, the expert noted that the graduated response system run by HADOPI has not led to a high number of condemnations. However, HADOPI is increasing the number of cases it brings to court. Moreover, according to the expert, the 3 million e-mails and 330,000 notice letters that the committee of Article L.331-25 IPC has sent between 2010 and 2014 appear to have caused a reduction in online copyright infringement.⁴⁵⁷

Regarding private enforcement, Article L.335-2-1 IPC prohibits the publishing, making available or communicating to the public of a computer program, manifestly intended to communicate unauthorized works or protected objects to the public, or encouraging the use of such software. This provision, which aims to fight unlawful downloading and communication infringements on the Internet, was central to the judgment of the Supreme Court of 25 September 2012. The case concerned Radioblog, who provided a computer program called RadioBlogClub to Internet users that enabled them to create a music player on an Internet page and to broadcast musical files in the form of playlists accessible to anyone via streaming. The Court condemned Radioblog and its managing directors to pay damages of a total amount of €1 million.⁴⁵⁸

In addition, in a 2018 judgement, the Supreme Court held that an access open to the public on the site of eMule is clearly intended to make available to the public the works and protected objects selected by the site, and therefore falls within the Article L.335-2-1 IPC. The Court explains that even though the site does not store the works, it presented on its homepage a kind of a guide for setting up and using the software.⁴⁵⁹

GERMANY

The most widely used and most effective enforcement measure in Germany is the cease-and-desist letter, a private enforcement measure (see *supra* at 4.1). To prevent an injunction granted by a court, the infringer has to enter into an obligation to desist from infringements, accompanied by equitable contractual penalties.⁴⁶⁰

NETHERLANDS

One of the most widely used enforcement measures in the Netherlands is the issuing of court orders to require Internet access providers to block access to infringing websites. Most of these orders have been initiated by *Stichting BREIN*, a private enforcement agency that represents large Dutch content industries. Probably the most high profile case is the case of *Stichting BREIN* against Internet access providers Ziggo and XS4ALL to block subscribers' access to *The Pirate Bay*. The case is currently

⁴⁵⁷ See also B. Spitz, 'Survey shows that the French graduated response fights online copyright infringement efficiently', *Kluwer Copyright Blog* (17 April 2018), available at <http://copyrightblog.kluweriplaw.com/2018/04/17/survey-shows-french-graduated-response-fights-online-copyright-infringement-efficiently/>.

⁴⁵⁸ Report France, citing Cass. com., 25 September 2012, 11-84224.

⁴⁵⁹ Report France, citing, the Supreme Court, 27 February 2018 (Criminal Chamber, No 16-86881).

⁴⁶⁰ Report Germany.

pending at the Dutch Supreme Court, which has to answer the case in accordance with the CJEU ruling in *Ziggo*.⁴⁶¹

In practice it is also common for Dutch intermediaries to employ voluntary NTD procedures, according to the aforementioned code of conduct in place for ISPs in the Netherlands (see *supra* at 4.1 and 4.2).

Furthermore, *Stichting BREIN* initiates civil enforcement actions against large-scale infringers if their identity can be obtained. Although some cases are reported to the public prosecutor, criminal copyright proceedings are infrequent in the Netherlands.⁴⁶²

POLAND

The most widely used measures against infringers in Poland are civil law injunctions and orders of damages based on the amount of double license fees. Sanctions against intermediaries are rare, but the expert reported a case from the Regional Court of Krakow. In this case, the court: (1) awarded damages under Article 422 of the Civil Code (intermediary as willful assisting users in committing a tort); and (2) imposed an injunction for future monitoring obligations regarding specific copyright works, namely checking hyperlinks to infringing content in Google and Bing search engines (based on Article 439 of the Civil Code on preventive liability).⁴⁶³

The defendant's appeal was largely dismissed by the Appeal Court in Kraków. The appeal court upheld the monitoring duties and extended the defendant's obligations by imposing a duty to remove or block access to accounts of repeat infringers. It should be, however, pointed out that the appeal court considered the defendant to be a direct rather than indirect (secondary) infringer. The main reason for this was the way the service provider was remunerated for downloads (downloading users had to pay downloading fees for each downloaded file separately). This change of perspective meant that the defendant could not invoke Articles 14 or 15 of the Polish E-Commerce Act.⁴⁶⁴ A cassation appeal has been filed by the defendant. The Supreme Court has not yet decided whether it will be heard.

SPAIN

The most widely used public enforcement measures against infringers include injunctions by the CPI (sec. 2) to remove and block access to infringing content, disconnect the Internet service of infringers and cancel or block access to ".es" domain names or infringing websites. In the (civil) *RojaDirecta* cases initiated by MediaPro and DTS/Movistar+, websites offering hyperlinks to sports events broadcasted by restricted access pay TV were condemned to close all infringing websites and pay damages to Movistar+. ISPs were ordered to block access to the infringing websites and to deny RojaDirecta any services concerning hosting or Internet access. RojaDirecta was also ordered to publish the ruling in two major Spanish newspapers and on the front page of its websites for two weeks.⁴⁶⁵

Criminal sanctions, introduced in 2015 to the Spanish Penal Code, are only recently starting to be issued and drawing media attention. For example, in *Youkioske*, the court imposed not only prison terms on infringers but also a number of enforcement measures, including the seizure of the computer

⁴⁶¹ Report Netherlands, citing relevant case law.

⁴⁶² Ibid.

⁴⁶³ Regional Court of Krakow, 27 May 2015, IX GC 791/12.

⁴⁶⁴ Report Poland, citing Judgment of September 18, 2017, case file no. I ACa 1494/15.

⁴⁶⁵ See Juzgado de lo Mercantil no. 2 de La Coruña, 22 November 2016, Westlaw.ES AC/2017/159, ECLI:ES:JMC:2016:4325, Audiencia Provincial de La Coruña, 26 April 2017, ECLI:ES:APC:2017:477A and Juzgado de lo Mercantil no. 1 de La Coruña, 1 February 2017, ECLI:ES:JMC:2017:5.

equipment in Madrid, an international injunction to close the website that was hosted in Canada and the blocking of the website through the Spanish ISPs.⁴⁶⁶

Finally, in an administrative procedure in 2015, all Spanish ISPs were ordered by the CPI (sec. 2) to suspend service and block access within 72 hours to any websites identified as belonging to *The Pirate Bay* group.⁴⁶⁷

SWEDEN

In Sweden, the information injunction constitutes a particularly effective measure for rights holders to receive all the necessary details for further proceedings. Usually a detailed cease-and-desist letter follows up in which the right holder threatens with litigation or seeks remuneration for specific use which has become known, hence combining public and private enforcement.⁴⁶⁸

Furthermore, right holders have also effectively initiated court proceedings against individuals, either through a civil or criminal case. In these cases, right holders were primarily interested in putting an end to the infringements and did not always seek damages or compensatory awards (also available in criminal cases). According to the expert, the use of public means of enforcement appears to be sufficiently effective, and it is noteworthy that public prosecutors are taking on cases involving mere sharing of content rather than restricting their activities to high-profile, commercial and large scale infringements.⁴⁶⁹

In 2017, a Swedish court issued the first ever injunction ordering an ISP to block its customers' access to a number of IP and http addresses relating to a website (*The Pirate Bay*), a development the expert attributes to the influence of the CJEU judgment in *UPC Telekabel*. The injunction ultimately awarded was for DNS blocking and targeted solely to one ISP, raising doubts as to effectiveness.⁴⁷⁰

UK

In the UK, injunctions against service providers under Section 97A CDPA appear to be widely used: more than 500 injunctions were granted according to 2015 numbers. Most of the case law applying Section 97A CDPA has concerned blocking injunctions. For instance, this type of injunction has been litigated in the cases concerning the live streaming of football matches and the unauthorized website *Popcorn Time*.⁴⁷¹

- Americas (Brazil and Canada)

BRAZIL

In Brazil, the measures that have shown to be most effective are those carried out directly against intermediaries as private enforcement, such as the sending of out-of-court notifications and in general the above described NTD system (supra at 3.3, 4.1 and 4.2). These measures are not established by law, but are important factors that courts take into account when deciding if an intermediary is subsidiary liable for copyright infringement. For instance, in a leading case on ISP liability for copyright infringement, the Superior Court of Justice established that an ISP can be held secondary

⁴⁶⁶ Report Spain, describing not only the *Youkioske* case but also the *Divxonline* case, which also involved inter alia imprisonment terms.

⁴⁶⁷ Ibid., citing JCCA no. 5 of Madrid, 25 March 2015 (*The Pirate Bay*).

⁴⁶⁸ Report Sweden, with further details and illustrative case law.

⁴⁶⁹ Ibid.

⁴⁷⁰ Patent and Market Court of Appeals 13 February 2017, 11706-15 (*The Pirate Bay*). NB the rightsholders in this case initiated proceedings only against one ISP. In other words, if the proceedings had been initiated against more ISPs, the blocking injunction would likely apply to those ISPs as well.

⁴⁷¹ Report UK, citing: EWHC 480 (Ch) 2017 Football Association Premier League/British Telecommunications; EWHC 1082 (Ch) 28 April 2015 Twentieth Century Fox Film Corporation/Sky UK (*Popcorn Time*).

liable if it does not make an URL to infringing material inaccessible after being notified by the interested party.⁴⁷² In another case, Google was ordered to pay material and moral damages to the author of the infringed works, on the grounds that it failed to remove the content immediately after obtaining knowledge of the illegality of the content.⁴⁷³

CANADA

In Canada, the most common enforcement measures against infringing users are infringement notices sent by right holders via intermediaries through the notice-and-notice system or by way of a Norwich order.⁴⁷⁴ Canadian copyright holders have sent millions of notices since the law came into force early 2015. Prior to the formal notice-and-notice provisions being enacted in 2015, there was an informal warning system between right holders and ISPs in place.⁴⁷⁵

The expert notes that copyright holders have not launched many civil infringement and anti-circumvention proceedings against users and intermediaries. In the few proceedings before Canadian courts, copyright holders have sought Norwich orders against ISPs and injunctions against sellers of infringing or circumventing technology. In a recent case from 2017, the Federal Court found that the defendant's mod chips circumvented Nintendo's TPMs and infringed copyright. The Court awarded Nintendo \$11.7 million in statutory damages for anti-circumvention, \$60 thousand in statutory damages for copyright infringement, \$1 million in punitive damages, the delivery up of the defendant's inventory and injunctions against the defendant's service.⁴⁷⁶

Finally, it is worth noting the current and controversial discussion in Canada on the possible implementation of a copyright web-blocking mechanism, to be managed by an independent third-party agency (the proposed Internet Piracy Review Agency), enforced by the the Canadian Radio-television and Telecommunications Commission (CRTC), and operating under the *Telecommunications Act*. As of writing, no decision regarding its implementation has been made.⁴⁷⁷

- Asia (Hong Kong, Indonesia, Japan, Thailand)

HONG KONG

The most widely used private enforcement measures are: (1) takedown notices issued to local and foreign online intermediaries; and (2) infringement notices issued to alleged infringers. If the infringers or intermediaries do not comply, court actions such as injunctions are usually taken. The most widely used public enforcement measure is reporting to (or cooperating with) the Hong Kong Customs and Excise Department. This Department has recently relied on the LMSI+ system to monitor popular online forums in Hong Kong and to track and arrest uploaders of audiovisual works. As the expert notes, the above measures are mainly matters of practice rather than measures of national law.⁴⁷⁸

INDONESIA

Regarding public enforcement, the expert notes that the most common measure is to file criminal complaints for copyright infringement. With sufficient evidence, public prosecutors follow these

⁴⁷² Report Brazil, citing STJ Recurso Especial 13 May 2015, no. 1.512.647, WWW <<https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1395049&tipo=0&nreg=201301628832&SeqCgrmaSessa o=&CodOrgaoJgdr=&dt=20150805&formato=PDF&salvar=false>>.

⁴⁷³ Ibid., citing STJ Agravo no Recurso Especial no. 259.482.

⁴⁷⁴ Report Canada, listing illustrative cases of Norwich Orders.

⁴⁷⁵ Ibid., mentioning the mass-scale practice by the company Canipre of sending notices on behalf of right holders.

⁴⁷⁶ Ibid, citing Nintendo of America Inc v. King, 2017 FC 246.

⁴⁷⁷ Ibid, Question 13. See also on this topic the extensive coverage by Michael Geist at <http://www.michaelgeist.ca/> (*The Case Against the Case Against Bell Coalition's Website Blocking Plan*, Parts 1 to 16).

⁴⁷⁸ Report Hong Kong.

through. As to private enforcement, a range of measures appears to be effective: civil remedies like damages, provisional measures (Anton Pillar Orders) and final injunctions (for discontinuation of infringement). In addition, the expert notes the administrative provisions under *Circular Letter No. 5 Year 2016* (see *supra* at 4.1) that allow for the possibility of closing a website following a report of an infringement to an ISP.⁴⁷⁹

It is also worth noting the existence of a new infringing website list made with the aim to reduce online piracy. The list was originally initiated in the UK by the Police Intellectual Property Crime Unit. It was introduced in Indonesia by the Creative Economy Agency (BEKRAF), the Indonesian Film Producers Association, Recording Company Association (ASIRI), the Indonesian Association of Advertising Agencies and the Motion Picture Association. The program aimed to identify the most popular piracy websites in Indonesia and encourage advertisers to remove their ads therefrom. It was reported in the media that at least 300 infringing websites on music were blocked as a result of this program.⁴⁸⁰ Recent data from the Motion Picture Association also suggests that “Site blocking has been successful in dramatically reducing traffic to targeted sites”.⁴⁸¹

Finally, as examples of the application of these measures in high profile cases over the last three years, the expert noted the use of provisional measures to stop the circulation of the “Soekarno” movie, which was successfully approved by the Central Jakarta Commercial Court in 2014,⁴⁸² as well as the closure of 21 Internet websites by the Minister of Communication and Information based on the report from Aprofi (Association of Indonesian Movie Producers) in 2015.⁴⁸³

JAPAN

The Japanese expert notes the existence of many court cases where copyright holders request from ISPs the disclosure of information on infringers under the regime of the ISP Liability Limitation Act (on which see *supra* at 4.4).⁴⁸⁴ It should also be noted that in April 2018 the Intellectual Property Policy Headquarters published the emergency plan against copyright infringing websites, encouraging ISPs to conduct site-blocking under certain conditions and announcing the establishment of a legal system to enable such site-blocking by ISPs.⁴⁸⁵

THAILAND

The most widely used enforcement practice is public criminal enforcement by police authorities. The expert notes that this is the most convenient and cost effective measure. Also common are direct warnings for the removal of infringing content, a private enforcement practice prior taking place before the start of a criminal procedure. The aforementioned enforcement measures against intermediaries under the Copyright Act and the Computer-Related Crime Act (*supra* at 4.1 and 4.2) have recently entered into force. Therefore, actual enforcement procedures have yet to be initiated. As an example of a recent high-profile case, the expert mentioned the closing of the website kodhit.com, a popular website on which Korean movies and series with Thai subtitles could be downloaded. The website was closed after it failed to respond to a takedown notice.⁴⁸⁶

⁴⁷⁹ Report Indonesia.

⁴⁸⁰ See <http://jakartaglobe.id/features/new-infringing-website-list-aims-to-reduce-online-piracy/>, regarding a new infringing website list aimed at reducing online piracy.

⁴⁸¹ See MPA, *Impact of Site Blocking in Indonesia* (October 2017), available at https://www.mpa-i.org/wp-content/uploads/2018/01/MPAA_Impact_of_Site_Blocking_in_Indonesia_Final.pdf.

⁴⁸² On which see IP Komodo Dragon, ‘Indonesia’s first civil search and seizure injunction’ (13 January 2014), available at <http://ipkomododragon.blogspot.nl/2014/01/indonesias-first-civil-search-and.html> and IP Komodo Dragon, ‘Trial and appeal leaves uncertainty over preliminary injunctions in Indonesia’, available at http://ipkomododragon.blogspot.nl/2015/03/trial-and-appeal-leaves-uncertainty_19.html

⁴⁸³ Report Indonesia.

⁴⁸⁴ Report Japan.

⁴⁸⁵ *Ibid.*, noting that the task-force meeting for this issue was to be established in June 2018.

⁴⁸⁶ Report Thailand, citing <http://www.manager.co.th/iBizChannel/ViewNews.aspx?NewsID=9590000115106>.

ANNEX 1: LEGAL QUESTIONNAIRE

[Questionnaire starts on the following page.]

Legal Questionnaire on Online Copyright Infringement

Instructions

Thank you for agreeing to participate in our legal questionnaire. We ask that you read all the *Instructions* and the *Annex* at the end of this document carefully before beginning the questionnaire. The *Annex* includes a glossary of technical terms, a list of abbreviations, and suggestions on style and drafting. You are encouraged to send any requests for clarification to j.p.quintais@uva.nl. (Subject: 'IViR Online Copyright Questionnaire').

The [Institute for Information Law](#) (IViR) of the University of Amsterdam is conducting an independent research project on *online copyright infringement*. Within the context of this project, we mean by this term the online use of protected music, films and TV series, books, and video games covered by an exclusive right (under copyright and related rights) but not authorized by the rights holders or otherwise permitted under the applicable law (e.g. by virtue of an exception or limitation). Online copyright infringement is also sometimes referred to as *online piracy*; this term is avoided here due to its lack of clarity.

The overall research project has three main aims. The first is to provide factual information about the state of online copyright infringement in different countries; the present legal questionnaire contributes to this part of the project. The second aim of the project is to assess the underlying motives and mechanisms of online copyright infringement, in particular its connection with enforcement measures and legal/authorized supply of the types of protected content mentioned above. The third is to assess the effect of online copyright infringement on consumption of protected content from legal/authorized sources.

The research project focusses on the impact of online copyright infringement on online and offline sales and consumption. It distinguishes four main online and offline channels to acquire or consume the types of content mentioned:

- Physical carriers (CD, DVD, blu-ray, print).
- Legal digital: downloading and streaming, free and paid-for.
- Live attendance to concerts and cinemas, as well as merchandise purchase.
- Illegal channels, such as unauthorized streaming websites, P2P platforms, cyberlockers, newsgroups, and *Kodi boxes*.

Within the larger research project, the purpose of this questionnaire is to gather legal information for each country studied. The focus of the questions is on quantitative and qualitative information that describes the legal situation of online copyright infringement in your country, including copyright enforcement by public authorities and rights holders.

The questionnaire consists of two main sections. The first section concerns the legal status of online copyright infringement and enforcement in your national law. This section includes questions on the relevant legal rules to address online copyright infringement under national law, as well as questions on enforcement measures, procedures, remedies and sanctions.

The second section focuses on content acquisition and consumption channels. This section seeks to identify prominent examples of legal/authorized and illegal/unauthorized websites and platforms providing online access to copyright-protected content in your country. Examples we hope you will be able to provide will be used as input for the country-specific examples in the consumer survey to be conducted at a later stage of the research project.

Questionnaire

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded **red**.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.⁴⁸⁷
2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?
3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
- Depends on the commercial or for-profit nature or intent of the use or user;
- Is uncertain and, if so, why;⁴⁸⁸
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

- a) Downloading copyright-protected content from illegal/unauthorized sources on the Internet.⁴⁸⁹
- b) **Streaming** copyright-protected content from illegal/unauthorized sources on the Internet.

⁴⁸⁷ This question does not require a description of the instruments or provisions identified.

⁴⁸⁸ For instance: the act is not clearly covered by exclusive rights, may be covered by an exception or limitation, may be subject to implied consent, the illegal/unauthorized nature of the source is unclear, or other.

⁴⁸⁹ For example, downloading a file with a song from a P2P platform such as The Pirate Bay would qualify as downloading from an illegal/unauthorized source. Differently, a legal/authorized source would be a service like iTunes in a country where that service has obtained the necessary authorizations from rights holders.

- c) **Stream-ripping** copyright-protected content.
 - d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.
 - e) Posting **hyperlinks** to copyright-protected content that has been made available online without the express authorization of the rights holder.
 - *Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard **surface hyperlink**, **deep-link**, **embedded or framing hyperlink**).*
 - f) The sale of **Kodi boxes** or similar devices.
 - g) Other types of unauthorized online use of copyright-protected content not listed above.
4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?⁴⁹⁰
5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country's law?⁴⁹¹ If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.⁴⁹²
6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:⁴⁹³

- The suspension from the Internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.

⁴⁹⁰ For instance: requirements for infringement may be different; parents may be considered liable for the acts of children; applicable remedies and sanctions may be different, etc.

⁴⁹¹ For example, in the EU, Arts 12 to 14 of the E-Commerce Directive include conditional liability exemptions (regarding claims for damages) to the benefit of intermediaries concerning the provision of services of 'mere conduit', 'caching', and 'hosting'.

⁴⁹² For instance: to what type of services they apply and subject to which conditions.

⁴⁹³ The examples listed here are taken from C. Angelopoulos, "European Intermediary Liability in Copyright" (Kluwer Law International 2016), pp. 465 et seq.

- The monitoring or **filtering** of content.
- The **blocking** and removing of infringing content, including notice-and-takedown⁴⁹⁴.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.⁴⁹⁵
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- **Graduated response systems.**

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

b) Administrative.

c) Criminal.

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law against intermediaries to address online copyright infringement by third party users of their services?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

b) Administrative.

c) Criminal.

9. To the best of your knowledge, are there significant differences in public and private enforcement practices⁴⁹⁶ depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

a) If yes, what conditions must be met for that obligation to arise?⁴⁹⁷

⁴⁹⁴ For example, Art. 14 of the E-Commerce Directive includes a notice-and-takedown system in the hosting safe-harbor.

⁴⁹⁵ For instance, the notices can be posted on the intermediary's terms and conditions, on the front-page of the platform, as a pop-up message for users of platform, etc. Cf. Angelopoulos 2016, op. cit., pp. 477–478.

⁴⁹⁶ In this question, enforcement 'practices' refers to the reality of enforcement on the field, including agreements between stakeholders for the enforcement of copyright online (e.g. codes of conduct for notice-and-take-down directed to ISPs that provide a public telecommunications service).

⁴⁹⁷ For example, is such disclosure only possible after a judicial court order, administrative proceedings, or simply at the request of rights holders?

- b) If yes, what type of personal data is typically requested?
11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?
12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?
- Please indicate whether the measures refer to public or private enforcement.⁴⁹⁸
- a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?
- b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.
13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.
14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions/campaigns aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?
15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?
16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

Annex to Legal Questionnaire

This Annex includes a glossary of technical terms used in the Questionnaire, a list of abbreviations that may be of use for filling out the Questionnaire, and a number of suggestions on style and drafting aimed at facilitating the analysis and aggregation of reports.

Glossary of Terms

⁴⁹⁸ In this context, ‘public enforcement’ refers to the use of public agents, agencies, bodies or authorities to detect and to sanction copyright infringers, whereas ‘private enforcement’ refers to the threat of litigation by private parties, namely rights holders or their representatives.

Blocking (of content)	The disabling of access for the intermediary's users to undesirable content. Blocking may take place at the point which the data is requested or at that at which it is sent; it may involve specifically identified communications, user accounts or entire websites. For search-engines, blocking is carried-out by 'de-indexing'.
Deep-link	A hyperlink to a sub-page or resource in the 'target' or 'destination' page.
Filtering	Monitoring measures with the objective of identifying unwanted content for subsequent blocking, removal or disposal.
Embedding or framing links	<p>'Embedded' links are links where the 'browser transparently fetches material (e.g., image or another web page) and displays it as part of the current page'. The link does not push the user from the source to the target page. Instead, the content stored in another website is 'pulled' and embedded in the source website, where it appears to users.</p> <p>In 'framing' links, the original web page address is preserved even when linking to external pages. The content is displayed in such a way as to appear part of the linking site, within a 'frame' (e.g., a pop-up window).</p>
Graduated response systems	Systems where ISPs monitor subscribers' potential illegal actions or act upon notification thereof, serving notices and warnings to subscribers to cease infringement. If users continue their practices after a number of warnings, sanctions are applied (e.g. suspension and termination of service, capping of bandwidth, and blocking of sites).
Hyperlink	Umbrella term encompassing similar types of references and means of access to other sources on the web. 'Standard' hyperlinks are clickable pointers, like text, a thumbnail or other format. Once clicked, the pointers cause the web browser to redirect or 'push' the user to a different 'target' or 'destination' page. A link to a main or homepage is called 'surface' linking.
Kodi Box	Multimedia player with pre-installed add-ons available online that contains hyperlinks to websites on which copyright-protected works or other subject-matter have been made available to the public.
Streaming	Method of transmitting data packets so that the earlier packets can be reassembled and processed before the entire file is downloaded, allowing for immediate display or playback. In essence, streaming involves downloading a file and subsequently causing the downloaded data to become inaccessible. Streaming can be linear (similar to a broadcast) or interactive/on-demand.
Stream ripping	Software tool that captures, aggregates, and saves all streaming data. The technology allows users to retain a permanent copy of the protected content streamed, making it equivalent to a download.

Abbreviations

Art.	Article
AG	Advocate General
BC	Berne Convention for the Protection of Artistic and Literary Works
Charter	Charter of Fundamental Rights of the European Union, OJ C 364/1, 18.12.2000

CJEU	Court of Justice of the European Union
E-Commerce Directive	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, 17.7.2000.
Enforcement Directive	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, 30.04.2004
EU	European Union
EUR	Euro (currency)
InfoSoc Directive	Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167/10, 22.06.2001
ISP	Internet Service Provider(s)
para. or paras	paragraph or paragraphs
P2P	Peer-to-peer
UK	United Kingdom
US	United States of America
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organization
WIPO Treaties	The WCT and WPPT
WPPT	WIPO Performances and Phonograms Treaty
WCT	WIPO Copyright Treaty

NB if you use specific abbreviations in your report (e.g. the current version of national Copyright Act), please identify them clearly on first use.

ANNEX 2: NATIONAL QUESTIONNAIRES – Responses to section 1 (online copyright infringement and enforcement in national law)

COUNTRY	NATIONAL EXPERTS AND AFFILIATION
France	DR. BRAD SPITZ, YS Avocats law firm (Paris)
Germany	PROF. DR. FRANZ HOFMANN, Lehrstuhl für Bürgerliches Recht, Recht des Geistigen Eigentums und Technikrecht Friedrich-Alexander-Universität Erlangen-Nürnberg
Netherlands	STEF VAN GOMPEL, Senior researcher and Lecturer, University of Amsterdam, Institute for Information Law
Poland	TOMASZ TARGOSZ, Institute of Intellectual Property Law, Jagiellonian University Kraków
Spain	RAQUEL XALABARDER, Professor, Chair of Intellectual Property, Universitat Oberta Catalunya
Sweden	KACPER SZKALEJ, Lecturer and PhD Candidate, Institute of Intellectual Property, Marketing and Competition Law (IMC), Uppsala University
United Kingdom	CHRISTINA ANGELOPOULOS, Lecturer, CIPIL, University of Cambridge
Brazil	ALLAN ROCHA DE SOUZA, Professor of Civil and IP law at UFRRJ/ITR Law School and of Copyright and Cultural Policy at the Graduation Program on Development and Public Policy (PPED/UFRJ), Researcher at INCT Proprietas, <i>and</i> LUCA SCHIRRU, PhD Candidate at the Graduation Program on Development and Public Policy (PPED/UFRJ). Researcher at INCT Proprietas. Lecturer in Copyright at PUC-RJ IP Course
Canada	DAVID FEWER, Executive Director Samuel-Glushko – CIPPIC (Centre for Law, Technology and Society), University of Ottawa
Hong Kong	ALICE LEE, Associate Dean (Academic Affairs) and Associate Professor, Faculty of Law, The University of Hong Kong
Indonesia	Dr. HENRY SOELISTYO, S.H., LL.M, Head, Master and Doctor of Law Program, Universitas Pelita Harapan. Jakarta
Japan	TATSUHIRO UENO, Professor of Law at Waseda University (Tokyo); Deputy Director of the Research Center for the Legal System of Intellectual Property (RCLIP) of Waseda University
Thailand	NING (NONTAYA) CHULAJATA and FABRICE MATTEI, Rouse Thailand

Note: for readability purposes, the explanatory footnotes to the questions in the Legal Questionnaire (available in ANNEX 1) are ommitted in the national questionnaires that follow.

Questionnaire France

DR. BRAD SPITZ, YS Avocats law firm (Paris)

Last updated: 1 June 2018

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded **red**.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.

Measures (withdrawal, filtering...) ordered by judges against computer programs and Internet services used for infringement acts

Graduated response system.

Use of an official label identifying the lawful websites.

2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?

Article 6 of the Act of 21 June 2004 on confidence in the digital economy (*‘loi sur la confiance dans l’économie numérique – LCEN’*) implements the Directive on electronic commerce, by establishing a system of limitation of liability of intermediary service providers, i.e. ISPs and hosting providers are defined in the Act. The Postal and Electronic Communications Code (*‘Code des postes et des communications électroniques’*) also defines ISPs.

Hosting providers are defined by Article 6-I-2 of the Act of 21 June 2004 as the persons who or legal entities that store, even without cost - for the provision of public services by public communication online - signals, texts, images, sounds or messages of any kind provided by the recipients of those services. Websites on which users can post content, such as YouTube, Dailymotion and Google, are hosting providers in the meaning of EU and French law. The limitation of liability will not apply to the information published or controlled by the hosting provider.

The hosting providers may not be held civilly liable as a result of the activities or information stored at the request of a recipient of services if they did not have actual knowledge of the unlawful nature,

nor of the facts and circumstances showing that nature, or if from the time they received this knowledge they acted promptly to remove the data or block access.

3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
- Depends on the commercial or for-profit nature or intent of the use or user;
- Is uncertain and, if so, why;
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

a) **Downloading copyright-protected content from illegal/unauthorized sources on the Internet.**

Downloading is subject to the reproduction right of the right holders (L.122-3 at the French intellectual property code “**IPC**”), and downloading from illegal/unauthorized sources qualifies as copyright infringement. Reproduction consists in the physical fixation of a work by any process permitting it to be communicated to the public in an indirect way.

The private copying exception does not apply, since two conditions will not be met in the framework of downloading: (1) the source of the copy is not lawful and (2) there are at least two people in the process. In other words, the latter condition (2) would make the act not private under French Law and, absent authorization, infringing.

Downloading will qualify as a copyright infringement whether it is of a commercial nature or not.

The legal qualification does not depend on its commercial or for-profit nature.

In civil cases, the infringer can be condemned without intent. However, in a criminal case, if the downloader is not considered as the main infringer, the existence of actual knowledge must be proved.

The type of protected content does not have an impact on whether the operation qualifies as copyright infringement.

b) **Streaming copyright-protected content from illegal/unauthorized sources on the Internet.**

Simply streaming (i.e. viewing as opposed to organizing the process) copyright-protected content from illegal/unauthorized sources on the Internet does not qualify as copyright infringement.

If the user only streams a work he/she will not be held liable of any copyright infringement. However, if the user uses a multimedia player that reproduces the works and that player does not benefit from the copyright exception for temporary reproduction, the situation would be similar to that described above in the answer to 3.a). In that case, French courts would follow the ECJ ruling in Case C-527/15 (*Filmsteler*) and the user could also be held liable for copyright infringement.

It should be added that certain authors of doctrine consider that Internet users streaming protected content could be prosecuted under criminal law for concealing, detaining or transmitting a product of

a crime or an offense (Article 321-1 of the Criminal Code), since the data is temporarily stored in the memory of the user's computer. But there is no conclusive case law on the matter, and liability would only concern criminal cases, and not civil cases. Moreover, in compliance with the Criminal Code, it would necessary to establish the user's intent and therefore his/her knowledge of the illicit nature of the content.

The type of protected content does not have an impact on whether the operation qualifies as copyright infringement.

c) Stream-ripping copyright-protected content.

Stream-ripping qualifies as a reproduction of the work and therefore will qualify as copyright infringement (see a).

In addition, Article L.331-5 IPC protects effective technological measures designed to prevent or restrict acts that are not authorized by holders of a copyright or a neighbouring right. Articles L.335-3-1 and L.335-3-2 IPC provide criminal sanctions in respect of infringement of the rights and obligations relating to the protection of technical measures.

Knowingly infringing, other than for research purposes, an effective technological measure in order to alter the protection of a work by decoding, decrypting or by any other personal intervention aimed at circumventing, disabling or removing a protective mechanism or control, is punished by a fine.

The type of protected content does not have an impact on whether the operation qualifies as copyright infringement.

d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.

Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder qualifies as a reproduction of the work and therefore will qualify as copyright infringement if it is carried out without the authorization of the rights holder (see a).

If the uploading in question has for sole purpose the communication to the public in the form of streaming, it would qualify as a communication to the public. However, it could also qualify, at the same time, as an act of reproduction. Indeed, in such a case, under French law it is possible that the act of uploading infringes both exclusive rights of reproduction and communication to the public.

The type of protected content does not have an impact on whether the operation qualifies as copyright infringement.

e) Posting **hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.**

- *Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard **surface hyperlink**, **deep-link**, **embedded or framing hyperlink**).*

The criteria set out by the ECJ in case C-160/15, *GS Media*, will be applied by the French courts, i.e. Article 3(1) of Directive 2001/29/EC must be interpreted as meaning that, in order to establish whether the fact of posting, on a website, hyperlinks to protected works, which are freely available on another website without the consent of the copyright holder, constitutes a 'communication to the public' within the meaning of that provision, it is to be determined whether those links are provided without the pursuit of financial gain by a person who did not know or could not reasonably have known the illegal nature of the publication of those works on that other website or whether, on the

contrary, those links are provided for such a purpose, a situation in which that knowledge must be presumed.

It does not seem that the French courts would distinguish between the different types of hyperlinking techniques.

The type of protected content does not have an impact on whether the operation qualifies as copyright infringement.

f) The sale of **Kodi boxes or similar devices.**

Under cases C-160/15 (*GS Media BV*) and C-527/15 (*Filmspeler*) which the French courts would apply in such cases, the sale of Kodi boxes or similar devices would qualify as a copyright infringement if such devices enable copyrighted-content that is available without the authorization of the copyright holders on the Internet to be freely accessed.

In addition, French copyright law provides for specific provisions that would apply to Kodi boxes and similar devices: Article L.335-2-1 IPC condemns publishing, making available or communicating to the public a computer program manifestly intended to communicate unauthorized works or protected objects to the public, or encouraging the use of such software.

The type of protected content does not have an impact on whether the operation qualifies as copyright infringement.

g) Other types of unauthorized online use of copyright-protected content not listed above.

The provisions of Article L.335-2-1 IPC (mentioned above) condemn publishing, making available or communicating to the public a computer program manifestly intended to communicate unauthorized works or protected objects to the public, or encouraging the use of such software. These provisions may be used to fight unlawful downloading and communication infringement on the Internet. E.g. a computer program that enables Internet users to create a music player on an Internet page and to broadcast musical files in the form of playlists accessible to anyone via streaming.

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

It should first be noted that the French IPC provides for criminal sanctions, but the victims may choose between the civil and the criminal procedures. In a civil procedure, no criminal sanctions may pronounced by the court.

In civil cases, there is no difference between the liability of the minor and that of the adult. However, the parents will be directly liable for the acts committed by their non-emancipated minor children.

In criminal cases, there is no minimum age set by law to incur criminal liability. All juveniles may be held accountable before the courts and brought before a judge. However, in each case, the judge has to assess the minor's discernment. The types of sanctions that may be pronounced by the courts will depend on the age of the minor.

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country's law? If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.

In France, the system provided for in Articles 12 et seq. of the E-Commerce Directive is implemented in Article 6 of the Act of 21 June 2004 on confidence in the digital economy and the Postal and Electronic Communications Code.

Article L.32-3-3 of the Postal and Electronic Communications Code states that ISPs may only incur civil or criminal liability in respect of the information transmitted if they are at the source of the request for the transmission, if they select the recipient of the transmission, or if they select or modify the content that is the object of the transmission.

Article 6-I-7 of the Act of 2004 provides that ISPs and hosting providers are not subject to a general obligation to monitor the information that they transmit or store, nor to a general obligation to seek facts or circumstances indicating illegal activity.

Article 6-I-2 of the Act of 21 June 2004 states that the hosting providers may not be held liable as a result of the activities or information stored at the request of a recipient of services if they did not have actual knowledge of the unlawful nature, nor of the facts and circumstances showing that nature, or if from the time they received this knowledge they acted promptly to remove the data or block access.

Article 6-I-5 of the Act of 21 June 2004 provides that the hosting provider is deemed to have actual knowledge of the relevant facts, and therefore will not benefit from the limitation of liability, when duly notified. The notice to take down must have the following elements:

- the date of the notification;
- if the applicant is a natural person: full name, profession, address, nationality, date and place of birth;
- if the applicant is a corporation: form, name, registered office and the body that legally represents the entity;
- the name and address of the recipient or, in the case of a corporation, its corporate name and registered office;
- the description of the litigious facts and their precise location (URL);
- the reasons for which the content should be removed, including the reference to legal provisions and evidence of the facts;
- a copy of the correspondence sent to the author or publisher of the litigious information or activities, requiring that the information be taken down or modified, or the reason why the author or the publisher could not be contacted.

Once the notification has been delivered, the hosting provider must take down the litigious content promptly, i.e. within one or two days.

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

No.

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:

- The suspension from the Internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.
- The monitoring or **filtering** of content.
- The **blocking** and removing of infringing content, including notice-and-takedown.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- **Graduated response systems**.

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

Infringement seizure: The copyright holders who wish to commission a bailiff ('huissier de justice') to search and secure evidence of an infringement act, may file a petition ('requête') before the President of the High Court of First Instance. The bailiff draws up a report called 'procès-verbal de constat', which is an authentic deed used as evidence.

Customs detention of goods at the request of the copyright holders: Under Article L.335-10 IPC, the customs authorities may, at the written request of an owner of copyright or a neighbouring right, withhold, in the course of its inspections, any goods the right holder alleges to be infringing.

Protective measures: In addition to the protective measures that may be ordered in application of the general procedural rules, the plaintiff may ask the court, during the pre-trial phase, to order the precautionary seizure of the capital assets and real estate of the alleged infringer. The claimant must demonstrate circumstances likely to jeopardize the recovery of damages. The court may, in particular, order the blocking of bank accounts and other assets.

Damages: Article L.331-1-3 paragraph 1 IPC provides that the court must, in order to assess the damages, take into account separately:

- the negative economic consequences of the infringement, including loss of profits and loss suffered by the injured party;
- the moral prejudice caused to the right holder;
- the profits made by the infringer, including savings in intellectual investment, equipment and promotion, which the infringer made through the infringement acts.

In certain situations the assessment of the prejudice will be difficult, especially if the right holder does not carry out the exploitation himself. Article L.331-1-3 paragraph 2 IPC offers an alternative to the assessment of the damages: the court may, as an alternative and at the request of the victim, award damages in a lump sum. This amount shall exceed the amount of royalties which would have been due if the infringer had requested the authorization to use the right which was infringed. This amount is not exclusive of compensation for the moral prejudice caused to the injured party.

The proceeds of the infringement: Article L.331-1-4 paragraph 4 IPC provides that the court may also, in addition to damages, order the confiscation of all or part of the proceeds that were made from the infringement of a copyright or a neighbouring right. This will be awarded to the victim or his assigns.

Confiscation and publicity: Article L.331-1-4 paragraphs 1 to 3 IPC provides that the court may, in its judgement, order additional remedies, at the expense of the party that is condemned for copyright or neighbouring rights infringement.

First, the court may order, at the request of the victim, the recall from the trade circuits, the destruction or the confiscation for the benefit of the victim, of the following elements: the objects made or manufactured in breach of the rights of the victim and the equipment predominantly used for the manufacture.

Second, the court may also order any appropriate measure to make the judgment public, including its display or its publication in full or in excerpts in newspapers or on the Internet.

b) Administrative.

1/

Customs detention of goods in the absence of a request from the copyright holder: Article L.335-11 IPC provides that in the absence of a written request from a right holder, the customs authorities may, within the framework of their control, withhold goods likely to infringe copyright or a neighbouring right (excluding perishable goods). The customs authorities inform the right holder, to whom pictures of the goods and information relating to the nature and the actual or estimated quantity are communicated. The prosecutor is also informed.

2/

The graduate response, which concerns the liability of Internet users, is partly administrative and partly criminal (as the users may be condemned to the payment of a fine).

The French legislator created a graduated system intended to stop the use of an Internet access connection for infringing purposes. The provisions and sanctions are extremely controversial and have been modified several times.

Article L.336-3 IPC provides that a person with access to Internet services has an obligation to ensure that his connection is not used for infringing reproductions or communications to the public. Until the Decree No. 2013-596 of 8 July 2013, the holders could be condemned to a suspension of their Internet access. This is no longer the case. The offence is not qualified as a misdemeanour and the only possible sanction is a simple fine of up to €1.5 thousand. The holder of an Internet access may be condemned if, without legitimate reason:

- he has not secured his access to Internet (e.g. by restricting access via the Wi-Fi system, thus avoiding a neighbour from using the access to download works unlawfully) or has lacked diligence in the implementation of the means to secure the access,
- he has been recommended, by letter and/or email, by the committee of Article L.331-25 IPC (HADOPI's *Commission de protection des droits*) to implement a means of securing access, and
- his access is used for infringing within the year following this recommendation.

These conditions are cumulative.

HADOPI is the High Authority for the Distribution of Works and the Protection of Rights on the Internet, created to supervise and implement the graduated response.

Moreover, Article 6-I-1 of the Act of 21 June 2004 on confidence in the digital economy states that ISPs have to provide information in their contracts with the subscribers on the provisions of Article L.336-3 IPC and on means to secure Internet access.

c) Criminal.

In compliance with Article 132-24 of the Criminal Code, the court will determine the sanction based on the nature of the offence and on the specific circumstances of the case. The sanctions provided in the IPC, and presented hereunder, therefore set out the maximum condemnations.

The following acts are punished by a three-year imprisonment and a fine of € 300 thousand: reproducing, communicating, making available to the public, broadcasting, on payment or free of charge, any performance, phonogram, videogram or program made without the authorization of the performer, that of the phonogram or videogram producer or that of the audiovisual communication undertaking, where such authorization is required.

The following acts are punishable by a fine of €300 thousand:

- Failing to pay the remuneration due to the author, the performer or the phonogram or videogram producer for private copying or public communication or the broadcasting of phonograms.
- Failing to pay the remuneration due for public lending.

Where the offences are committed by an organised criminal group, the penalties are increased to five-year imprisonment and a fine of €500 thousand.

Article L.335-2-1 IPC condemns publishing, making available or communicating to the public, knowingly and in any form whatsoever, a computer program manifestly intended to communicate unauthorized works or protected objects to the public, or encouraging the use of such software, with up to 3 years imprisonment and a fine of up to €300 thousand.

Infringing the rights and obligations relating to the protection of technical measures is condemned by Articles L.335-3-1 and L.335-3-2 IPC.

Closure of the establishment: The court may order the total or partial, permanent or temporary closure, for a period not exceeding five years, of the establishment that has served for the commission of the offence.

Confiscation, destruction and publicity: The court may order the confiscation of the equipment and materiel installed for the purpose of committing the offence. The court may also order, at the cost of the convicted person, the publication of the judgment.

Suspension of Internet access: Article L.335-7 IPC provides that when the offence is committed using an online service, persons convicted may also be sentenced to the additional penalty of suspension of access to Internet, for a maximum of one year. During that period, the persons are prohibited from entering into another contract for the same service with any operator. When this service is part of a commercial package including other types of services, such as phone services or television, the suspension does not apply to these services. The costs of a possible termination of the subscription during the period of suspension are borne by the subscriber. When the court's decision becomes enforceable, the sanction is brought to the attention of the High Authority (HADOPI), which shall

notify the ISP. If the ISP does not suspend the services within 15 days of the notification, it may be punished by a fine of up to €5 thousand.

Sanctions specific to legal entities: The legal entities declared criminally liable for any infringement act mentioned above, may be condemned to:

- a fine up to five times that provided for natural persons by the law which punishes the offence, and
- the liquidation of the legal entity, the prohibition to exercise an activity, the judicial supervision, the exclusion from public contracts.

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law against intermediaries to address online copyright infringement by third party users of their services?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

It should first be noted that if an intermediary may not rely on the liability exemption system (e.g. it does not promptly remove copyrighted content after receipt of a notification), the measures and remedies described above will apply.

Computer programs used for infringement acts (such as P2P software): Article L.336-1 IPC provides that if a computer program is mainly used for unlawfully making available subject-matters protected by copyright or a neighbouring right, the President of the High Court of First Instance may, ruling in summary proceedings, order under penalty all necessary measures to protect this right in accordance with the state of the art. The measures ordered may not have the effect of undermining the essential characteristics or the original destination of the computer program. Measures ordered may possibly consist of the implementation of devices such as filtering processes, which would prevent or make it more difficult to carry out the unlawful acts.

Internet services used for infringement acts: Article L.336-2 IPC provides that in the presence of an infringement of a copyright or related right caused by the content of an Internet service, the High Court of First Instance, if appropriate acting in the form summary proceedings, may, at the request of the right holders, collecting societies or trade unions, order any person likely to remedy the situation to implement measures to prevent or to block the infringement acts.

The French Supreme Court ruled that the French Union of Phonographic publishing (SNEP) could request that Google be ordered to remove certain suggestions from its 'Google Suggest' service, which automatically presents popular searches while the Internet user types his search (Cass. civ. 1, 12 July 2012, 11-20358).

Finally, on the related matter of costs for the application of enforcement measures, in a judgement of 6 July 2017 (Nos 16-17217, 16-18298, 16-18348, 16-18595), the French Supreme Court held that the costs relating to the blocking measures ordered by the courts are strictly necessary for the preservation of the intellectual property rights and that the courts may order the ISPs and search engine providers to bear such costs.

b) Administrative.

c) **Criminal.**

It should be noted that if an intermediary may not rely on the liability exemption system (e.g. it does not promptly remove copyrighted content after receipt of a notification), the measures, criminal sanctions and remedies described above will apply.

9. To the best of your knowledge, are there significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

No.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

Yes.

a) If yes, what conditions must be met for that obligation to arise?

Article 6-II of Act No. 2004-575 of 21 June 2004 on confidence in the digital economy provides that ISPs and hosting providers have an obligation to hold and conserve data (for a period of 1 year) that will lead to the identification of anyone who has contributed to the creation of content.

The judicial authorities may require that they communicate such information. This enables the victims of infringement acts to ask the President of the High Court of First Instance to issue an order to communicate the information (name, IP address, etc.). Given the nature of the information, and the fact that the information is processed personal data, it is not possible to simply request this information directly from the ISP or hosting provider.

b) If yes, what type of personal data is typically requested?

Article 1 of Decree of 25 February 2011 “on the conservation and communication of data allowing the identification of any person who contributed to the creation of content published online” specifies the information to be kept:

- The types of protocols used to connect to the service and to transfer the contents.
- The information provided during the subscription of a contract by a user or during the creation of an account: the username of this connection at the time of the creation of the account; name and surname or business name; the associated postal addresses; the pseudonyms used; the associated e-mail or account addresses; telephone numbers.

These are the personal data typically requested to the hosting providers, along with the IP addresses that will enable the claimant to then ask the ISPs (via a judicial order) for the information relating to the user if the latter has provided incorrect information to the hosting provider.

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

The copyright holders and the judicial and police authorities.

French law is consistent Article 4 of the Enforcement Directive, meaning that in the circumstances prescribed in the law also licensees, CMOs, and professional defence bodies are entitled to apply for civil measures.

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

- Please indicate whether the measures refer to public or private enforcement.

Public enforcement: There are few condemnations under the graduate response described hereinabove at 7-b-2. However, HADOPI is increasing the number of cases it brings to court (688 between June 2015 and June 2016, compared with 362 between 2010 and June 2015).

Moreover, the emails and notice letters that the committee of Article L.331-25 IPC has sent seem to have had a positive impact on reducing the numbers of users who use the Internet to download works and other subject-matters unlawfully (over 3 million emails and over 330,000 letters sent between 2010 and 2014).

Private enforcement: Article L.335-2-1 IPC which condemns publishing, making available or communicating to the public a computer program manifestly intended to communicate unauthorized works or protected objects to the public, or encouraging the use of such software, may be used to fight unlawful downloading and communication infringement on the Internet. Example of a high profile cases:

- Supreme Court (Cass. com., 25 September 2012, 11-84224) upheld the appeal judgement that condemned to € 1 million in damages an Internet company, Radioblog, and its managing directors, on the grounds of Article L.335-2-1 IPC. The website Radioblog provided a computer program called 'RadioBlogClub' to Internet users that enabled them to create a music player on an Internet page and to broadcast musical files in the form of playlists accessible to anyone (via streaming).
- Supreme Court (Criminal Chamber, No 16-86881, 27 February 2018) held that an access open to the public on the site of eMule is clearly intended to make available to the public the works and protected objects selected by the site, and therefore falls within the Article L.335-2-1 IPC. The Court explains that even though the site does not store the works, it presented on its homepage a kind of a guide for setting up and using the software

a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?

No.

b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.

See above.

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

The recent cases of the European Court of Justice on hyperlinks (cases C-466/12, *Svensson*; C-160/15, *GS Media*; and C-527/15, *Filmspeler*) have caused a stir in France. In legal reviews, authors of doctrine are concerned by the fact that the rulings do not set clear rules. In specialized Internet reviews, authors have written that they are worried that *GS Media* endangers hypertext linking.

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions/campaigns aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

No.

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

Under Articles L. 331-13 and L. 331-23 IPC, HADOPI has created an official label identifying the lawful websites, called “Offre Légale” (lawful offer). The label identifies the lawful websites on said sites, and are listed and presented on the website of HADOPI: <https://www.offrelegale.fr/sites-et-services>

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

<https://offrelegale.fr/statistiques/toutes-les-categories>

Questionnaire Germany

PROF. DR. FRANZ HOFMANN, Lehrstuhl für Bürgerliches Recht, Recht des Geistigen Eigentums und Technikrecht Friedrich-Alexander-Universität Erlangen-Nürnberg

Last updated: 1 June 2018

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded **red**.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.

Private enforcement

- *Section 97 Act on Copyright and Related Rights*: Right to require cessation of infringement (injunctions) and to damages (including compensation for non-pecuniary damages = *Section 97 (2) Sentence 4*)
- *Section 97a Act on Copyright and Related Rights*: Notification (= “Abmahnung”)
- *Section 98 Act on Copyright and Related Rights*: Claim to destruction, recall and release of copies
- *Section 100 Act on Copyright and Related Rights*: Pecuniary compensation (damages in lieu of an injunction)
- *Section 101 Act on Copyright and Related Rights*: Right of information
- *Section 101a Act on Copyright and Related Rights*: Entitlement to presentation and inspection
- *Section 101b Act on Copyright and Related Rights*: Securing claims for damages
- *Section 103 Act on Copyright and Related Rights*: Publication of judgment
- *Section 687 German Civil Code*: False agency without specific authorization
- *Section 812 German Civil Code*: Claim for restitution (unjust enrichment = restitution for wrongs)
- *Section 823 (2) German Civil Code*: Liability in damages (in conjunction with *Section 95a Act on Copyright and Related Rights*: Protection of technological measures)
- *Section 826 German Civil Code*: Intentional damage contrary to public policy
- *Section 3 Act Against Unfair Competition*: Prohibition of unfair commercial practices (probably not applicable, German Federal Court, 19.11.2015 – I ZR 149/14 – *Pippi Langstrumpf-Kostüm II*)
- *Section 4 No. 3 Act Against Unfair Competition*: Protection of competitors

Criminal provisions

- *Section 106 Act on Copyright and Related Rights*: Unlawful exploitation of copyrighted works

- *Section 107 Act on Copyright and Related Rights*: Unlawful affixing of designation of author
- *Section 108 Act on Copyright and Related Rights*: Infringement of related rights
- *Section 108a Act on Copyright and Related Rights*: Unlawful exploitation on a commercial scale
- *Section 108b Act on Copyright and Related Rights*: Infringement of technological measures and rights-management information
- *Section 109 Act on Copyright and Related Rights*: Application for criminal prosecution
- *Section 110 Act on Copyright and Related Rights*: Confiscation
- *Section 111 Act on Copyright and Related Rights*: Publication of judgement

Regulatory fine provisions

- *Section 111a Act on Copyright and Related Rights*: Regulatory fine provisions

Provisions on measures taken by the customs authorities

- *Section 111b Act on Copyright and Related Rights*: Proceedings under German law
- *Section 111c Act on Copyright and Related Rights*: Proceedings according to Regulation (EU) No 608/2013

2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?

Intermediaries can be liable according to *Section 1004 German Civil Code* (Claim for injunction). More precisely, liability of intermediaries is based on the concept of “interferer liability” (“*Störerhaftung*”), which has been shaped by case law. Any person who has willfully made a causal contribution to the direct copyright infringement by a third party can be held liable for injunctive relief if the contributor has violated a reasonable duty of care to prevent such direct infringements. Those principles are applicable to all kind of intermediaries. Damages are not available.

Contributory liability (*Section 830 German Civil Code*: Joint tortfeasors and persons involved) depends on the intent of the intermediary. In the majority of cases, liability cannot be established. The intermediary regularly has no knowledge of the specific copyright infringement by a third party.

Arts 12 – 15 E-Commerce Directive (2000/31/EC) are implemented in **Secs 7 – 10 Tele-Media Act** (*Telemediengesetz*)

- Section 7 Tele-Media Act: General Principles (= Art. 15 (1) E-Commerce Directive)
- Section 8 Tele-Media Act: Mere conduit
- Section 9 Tele-Media Act: Caching
- Section 10 Tele-Media Act: Hosting

3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
- Depends on the commercial or for-profit nature or intent of the use or user;
- Is uncertain and, if so, why;
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

a) Downloading copyright-protected content from illegal/unauthorized sources on the Internet.

Downloading copyright-protected content from illegal/unauthorized sources infringes the right of reproduction (*Section 16 Act on Copyright and Related Rights*). However, the reproduction might be covered by the limitation set out in *Section 53 Act on Copyright and Related Rights*. Section 53 provides an exception with respect to reproductions for private and other personal uses. Particularly: Making single copies for private purposes does not constitute a copyright infringement as long as the source is not obviously illegal.

In detail *Section 53: Reproduction for private and other personal uses* provides:

Section 53: Reproduction for private and other personal uses

(1) It shall be permissible for a natural person to make single copies of a work for private use on any medium, insofar as they neither directly nor indirectly serve commercial purposes, as long as no obviously unlawfully-produced model or a model which has been unlawfully made available to the public is used for copying. A person authorised to make copies may also cause such copies to be made by another person if no payment is received therefore, or if it involves copies on paper or a similar medium which have been effected by the use of any kind of photomechanical technique or by some other process having similar effects.

(2) It shall be permissible to make single copies of a work or to have these made

- 1. for one's own scientific use if and to the extent that such reproduction is necessary for the purpose and it does not serve a commercial purpose,*
- 2. for inclusion in a personal archive if and insofar as the reproduction is necessary for this purpose and one's own personal copy of the work is used as the model from which the copy is made,*
- 3. for one's own personal information concerning current affairs if the work was broadcasted,*
- 4. for other personal use*

a) in the case of small parts of a released work or individual articles being released in newspapers or periodicals,

b) in the case of a work which has been out of print for at least two years.

This shall apply in the case under the first sentence, number 2 only if in addition,

- 1. the reproduction is effected on paper or any similar medium by the use of any kind of photographic technique or by some other process having similar effects, or*
- 2. exclusively analogue use takes place, or*
- 3. the archive acting in the public interest and pursues no direct or indirect economic or commercial purpose.*

This shall apply in the cases referred to under the first sentence, numbers 3 and 4 only if in addition one of the conditions under the second sentence, numbers 1 or 2 pertains.

(3) It shall be permissible to make copies for personal use of small parts of a work, of small-scale works or of individual articles released in newspapers or periodicals or made available to the public

- 1. for the purpose of illustration for teaching in schools, in non-commercial training and further training institutions, as well as vocational training institutions in quantities required for the persons receiving instruction, or*
- 2. for state examinations and examinations in schools, higher education institutions, non-commercial training and further training institutions, as well as vocational training institutions in the required quantity,*

or to have these copies made if and insofar as reproduction is necessary for this purpose. The reproduction of a work intended for instructional use at schools shall be permissible only in cases where the person entitled has given his consent.

(4) The reproduction of

- a) graphic recordings of musical works,*
- b) a book or a periodical, in the case of an essentially complete reproduction,*

shall, insofar as this does not occur by means of manual transcription, always be permissible only with the consent of the rightholder or under the conditions in accordance with subsection (2), first sentence, number 2, or for personal use if, the work has been out of print for at least two years.

(5) Subsection (1), (2), first sentence, numbers 2 to 4, as well as subsection (3), number 2, shall not apply to database works the elements of which are individually accessible by electronic means. Subsection (2), first sentence, number 1, as well as subsection (3), number 1, shall apply to such database works on condition that the scientific use or use in instruction does not serve commercial purposes.

(6) The copies may neither be distributed nor communicated to the public. It shall, however, be permissible to lend lawfully produced copies of newspapers and out-of-print works, as well as those works in which no damaged or missing parts have been replaced by means of copies.

(7) The recording of public lectures, productions or performances of a work on video or audio recording mediums, the realisation of plans and drafts of artistic works and the reconstruction of architectural works shall always be permissible only with the consent of the rightholder.

b) Streaming copyright-protected content from illegal/unauthorized sources on the Internet.

Downloading copyright-protected content from illegal/unauthorized sources infringes the right of reproduction (*Section 16 Act on Copyright and Related Rights*). Art. 16 (1) provides: The right of reproduction is the right to produce copies of the work, **whether on a temporary** or on a lasting basis and regardless of by which means of procedure or in which quantity they are made.

But there are limitations: Section 53 is applicable. Consequently, streaming for private use does not infringe copyright as long as the source is not obviously illegal.

Whether Section 44a *Act on Copyright and Related Rights* (Temporary acts of reproduction = Art. 5 (1) InfoSoc Directive) covers streaming from illegal sources is uncertain. On the one hand some argue that “lawful use” (Sec. 44a No. 2) has to be interpreted in the sense, that mere consumption of works is allowed. Like reading a book, streaming a video is qualified as such a lawful use. On the other hand, some draw an analogy to Sec. 53 (1): Only if the source is not obviously illegal, streaming copyright protected material available on the Internet constitutes copyright infringement. Probably, after the CJEU decision C-527/15 – *Stichting Brein/Jack Frederik Wullems (Filmspeler)* national law will take the latter view.

c) Stream-ripping copyright-protected content.

With respect to downloading, see *supra*.

Depending on the facts of the case stream-ripping might qualify as interference with Section 95a *Act on Copyright and Related Rights*, which protects technological measures.

Section 95a provides:

“(1) Effective technological measures to protect a work protected under this Act or other subject-matter protected under this Act may not be circumvented without the consent of the rightholder where the person acts in the knowledge or with reasonable grounds to know that circumvention is taking place in order to facilitate access to such a work or protected subject-matter or its use.

(2) For the purpose of this Act, technological measures shall be technologies, devices and components which, in the normal course of their operation, are designed to prevent or restrict acts, in respect of protected works or other subject-matter protected pursuant to this Act, which are not authorised by the rightholder. Technological measures shall be deemed effective where the use of a protected work or of other subject-matter protected pursuant to this Act is controlled by the rightholder through application of an access control, a protection process, such as encryption, scrambling or other transformation, or a copy control mechanism, which achieves the protection objective.

(3) The production, import, distribution, sale, rental, advertising with a view to selling or rental and possession for commercial purposes of devices, products or components, as well as providing services, shall be prohibited which

- 1. are the subject-matter of sales promotions, advertising or marketing with the aim of circumventing effective technological measures, or*
- 2. apart from circumventing effective technological measures only have a restricted economic purpose or benefit, or*
- 3. are mostly drafted, produced, adjusted or provided in order to facilitate or make easier the circumvention of effective technological measures.”*

Remedies available would be injunctions and damages.

d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.

This constitutes a copyright infringement according to Section 19a *Act on Copyright and Related Rights*. Section 19a provides: The right of making works available to the public shall constitute the right to make the work available to the public, either by wire or wireless means, in such a manner that members of the public may access it from a place and at a time individually chosen by them.

Limitations and exceptions are not applicable.

e) Posting **hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.**

Links (surface hyperlink, deep-link etc.) which allow users of the website on which it is posted to circumvent the restrictions taken by the site where the protected work is posted constitutes an infringement of the right of making works available to the public (Sec. 19a; German Federal Court, 29.4.2010 – I ZR 39/08 – *Session-ID*).

Posting a hyperlink to copyright-protected works, which are freely available on another website without the consent of the copyright holder, constitutes a ‘communication to the public’ according to Section 15 (2) *Act on Copyright and Related Rights* which provides:

“The author further has the exclusive right to communicate his work to the public in non-material form (right of communication to the public).” (see OLG München, 25.8.2016 – 6 U 1092/11 – Die Realität III; BGH, 9.7.2015 – I ZR 46/12 para. 34 – Die Realität II)

After the CJEU decision *GS Media* C-160/15 the regional court Hamburg held (LG Hamburg, 18.11.2016 – 310 O 402/16 – *Architekturfotos*) that posting a hyperlink to copyright-protected content available online without the consent of the rights holder constitutes a copyright infringement if the link is posted on a commercial website and the person posting the link knew or had to know that the

rights holder had not authorized the publication on the Internet. The right of making works available to the public (Sec. 19a) was violated.”

Recently the German Federal Court had to decide a case concerning links in the context of search engines (German Federal Court: BGH, Urt. V. 21.9.2018 – I ZR 11/16). The defendant offered a search function on his website. As he couldn’t provide the service himself, he cooperated with a search engine. While the search was executed by the third party search engine, the defendant provided hyperlinks to the results which the search engine had delivered. The dispute concerned thumbnails of pictures which were available on the internet without the consent of the copyright holder. The German Federal Court ruled that the defendant did not infringe copyright. In case of search engines there is no presumption that the user has knowledge whether the respective content has been published with the consent of the copyright holder or not.

- Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard *surface hyperlink*, *deep-link*, *embedded or framing hyperlink*).

The answers given do not vary depending on the type of hyperlinking technique.

f) The sale of *Kodi boxes* or similar devices.

A person who sells Kodi boxes or similar devices could be liable for contributing to copyright infringements depending on his knowledge. The “interferer liability” (“Störerhaftung”) could be applicable too. However, the German Federal court has not decided such cases yet. After the decision CJEU decision C-527/15 – Stichting Brein/Jack Frederik Wullems (*Filmspeler*) national law will probably qualify the sale of Kodi boxes or similar devices as communication to the public.

g) Other types of unauthorized online use of copyright-protected content not listed above.

Nothing to report.

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

The liability for copyright infringement by minors is restricted. Section 828 *German Civil Code* (Minors) is applicable.

Section 828 Minors

(1) A person who has not reached the age of seven is not responsible for damage caused to another person.

(3) A person who has not yet reached the age of eighteen is, to the extent that his responsibility is not excluded under subsection (1) or (2), not responsible for damage he inflicts on another person if, when committing the damaging act, he does not have the insight required to recognise his responsibility.

Parents are liable according to Section 832 *German Civil Code*:

Section 832 Liability of a person with a duty of supervision

A person who is obliged by operation of law to supervise a person who requires supervision because he is a minor or because of his mental or physical condition is liable to make compensation for the damage that this person unlawfully causes to a third party. Liability in

damages does not apply if he fulfils the requirements of his duty to supervise or if the damage would likewise have been caused in the case of proper conduct of supervision.

According to the German Federal Court (BGH, 15.11.2012 – I ZR 74/12 – Morpheus) parents have to explain copyright law to their children. However, there is no obligation to monitor the children's Internet use.

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country's law? If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.

As mentioned above Arts 12 – 15 E-Commerce Directive (2000/31/EC) are implemented in Secs 7 – 10 Tele-Media Act.

Section 7: General principles

(1) Service providers shall be responsible for their own information which they keep ready for use, in accordance with general legislation.

(2) Service providers within the meaning of Sections 8 to 10 are not required to monitor the information transmitted or stored by them or to search for circumstances indicating an illegal activity.

(3) This shall be without prejudice to obligations to remove or disable access to information pursuant general laws due to court order or official directive, even where the service provider does not bear responsibility pursuant to Sections 8 to 10. Privacy of telecommunications pursuant to Section 88 of the Telecommunications Act must be maintained.

(4) Should a user of a service have utilized a tele-media service in order to infringe intellectual property rights of third parties, with no other possibility for the holder of the right to remedy the infringement, the holder of the right may seek to disable the use of the information by the concerned service provider pursuant to Section 8 (3) in order to prevent further repetition of such an infringement. The disablement shall be reasonable and proportionate. The holder of the right shall not be entitled to any refund of all extra-judicial costs for enforcement of the claim pursuant to sentence 1 from the service provider except in cases of Section 8 (1) sentence 3.

Section 8: Acting as a conduit of information

(1) Service providers shall not be responsible for the information of third parties which they transmit in a communication network or to which they give access, as long as they

- 1. have not initiated the transmission,*
- 2. have not selected the addressee of the transmitted information, and*
- 3. have not selected or modified the transmitted information.*

As long as service providers are not responsible they shall particularly not be claimed liable for damages or removal or injunction due to a illegal activity of a user; idem applies to all costs of enforcement of the claim. Sentence 1 and 2 shall not apply when the service provider deliberately works together with a recipient of his service to commit illegal acts.

(2) The transmission of information pursuant to Subsection 1 and the provision of access to it includes the automatic, intermediate and transient storage of this information, in so far as this takes place for the sole purpose of carrying out the transmission in the communication network and the information is not stored for any period longer than is reasonably necessary for the transmission.

(3) Subsection 1 and 2 shall also apply for service providers within the meaning of subsection 1, who provide users access to the internet via a wireless local area network.

(4) Pursuant to Section 8 (3) service providers may not be obliged by an authority

1. before granting access
 - a) to collect personal information from users and store them (registration) or
 - b) to require the entry of a password or
2. to cease offering the service permanently.

This has no effect when a service provider voluntarily identifies users, requires a password entry or takes other voluntary measures.

Section 9: Temporary storage for the accelerated transmission of information

Service providers shall not be responsible for automatic, intermediate and temporary storage which serves the sole purpose of making more efficient the information's onward transmission to other recipients on their request, as long as they

1. do not modify the information,
 2. comply with conditions on access to the information,
 3. comply with rules regarding the updating of the information, specified in a manner widely recognised and used by industry,
 4. do not interfere with the lawful use of technology, stipulated in widely recognised and used industrial standards, to obtain data on the use of the information, and
 5. act expeditiously to remove or to disable access to the information they have stored within the meaning of this provision upon obtaining knowledge of the fact that the information at the initial source of the transmission has been removed from the network or that access to it has been disabled, or that a court or administrative authority has ordered such removal or disablement.
- Section 8 (1) sentence 2 applies mutatis mutandis.

Section 10: Storing of information

Service providers shall not be responsible for the information of third parties which they store for a recipient of a service, as long as

1. they have no knowledge of the illegal activity or the information and, as regards claims for damages, are not aware of any facts or circumstances from which the illegal activity or the information is apparent, or
2. upon obtaining such knowledge, have acted expeditiously to remove the information or to disable access to it.

Sentence 1 shall not apply when the recipient of the service is acting under the authority or control of the service provider.

Practically, Section 7 (2) Sentence 1 Tele-Media Act is important: Service providers within the meaning of Sections 8 – 10 have no general obligation to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating an illegal activity. The safe harbor provisions are important within the concept of “interferer liability”. The safe harbor provisions are discussed with respect to the question whether an intermediary has violated a reasonable duty of care to prevent a direct copyright infringement. As a result, within the concept of “interferer liability” (“Störerhaftung”) both host providers and access-providers only have to react if they have been informed about the infringement (notice-and-take-down).

See question 6 *infra*.

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

German law differentiates between own content and external content (=information of third parties). With respect to own content there are no safe-harbor provisions (see Section 7 (1) Tele-Media Act). Intermediaries are liable for copyright infringements according to general principles. With the respect to external content Sections 8 – 10 Tele-Media Act are applicable.

The line between own content and external content is difficult to draw. The German Federal Court says: Content is to be considered as own content if the intermediary takes on responsibility for the content published on his website. Whether that is the case or not has to be assessed on the facts of the case based on the perspective of an average user (BGH, 12.11.2009 – I ZR 166/07 marions-kochbuch.de)

For example, it is highly controversial whether the content on YouTube has to be considered as content for which YouTube is primarily responsible (own content) or whether the liability has to be established according to the principles of “interferer liability” (“Störerhaftung”), see OLG München, 28.1.2016 – 29 U 2798/15 – Allegro barbaro.

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:

- The suspension from the Internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.
- The monitoring or **filtering** of content.
- The **blocking** and removing of infringing content, including notice-and-takedown.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary’s services cannot be used for its commission.
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- **Graduated response systems.**

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country’s law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

Remedies against individuals who infringe copyright online (see above question 1):

- *Section 97 Act on Copyright and Related Rights*: Right to require cessation of infringement (injunctions) and to damages (including compensation for non-pecuniary damages = *Section 97 (2) Sentence 4*)
- *Section 97a Act on Copyright and Related Rights*: Notification (= “Abmahnung”)
- *Section 98 Act on Copyright and Related Rights*: Claim to destruction, recall and release of copies

- *Section 100 Act on Copyright and Related Rights*: Pecuniary compensation (damages in lieu of an injunction)
- *Section 101 Act on Copyright and Related Rights*: Right of information
- *Section 101a Act on Copyright and Related Rights*: Entitlement to presentation and inspection
- *Section 101b Act on Copyright and Related Rights*: Securing claims for damages
- *Section 103 Act on Copyright and Related Rights*: Publication of judgment

- *Section 687 German Civil Code*: False agency without specific authorization
- *Section 812 German Civil Code*: Claim for Restitution (unjust enrichment = restitution for wrongs)
- *Section 823 (2) German Civil Code*: Liability in damages (in conjunction with *Section 95a Act on Copyright and Related Rights*: Protection of technological measures)
- *Section 826 German Civil Code*: Intentional damage contrary to public policy

There are no differences depending on the type of protected content.

In any case, right holders can start legal proceedings. However, where the defendant has not given cause for an action to be brought, the plaintiff shall bear the costs of the proceedings should the defendant immediately acknowledge the claim.

Section 93 Code of Civil procedure: Costs in the event an immediate acknowledgment is made

Where the defendant has not given cause for an action to be brought, the plaintiff shall bear the costs of the proceedings should the defendant immediately acknowledge the claim.

For that reason, right holders should in the first place try to settle their claims out of court. With regard to the right to require cessation (enforced by an injunction) right holders are well-advised to send a “cease-and-desist letter” to the direct or indirect infringer. This procedure is addressed in *Section 97a Act on Copyright and related rights*.

Section 97a Notification

(1) The injured party shall notify the infringer before instituting proceedings in court to desist from infringement and shall give him the opportunity to settle the dispute by entering into an obligation to desist from infringement accompanied by an equitable contractual penalty.

(2) The notification shall clearly and comprehensibly

1. state the name or company of the injured party if it is not the injured party but a representative who gives notification,

2. provide a precise description of the infringement,

3. break down claims to payment asserted into claims for damages and claims for compensation, and

4. if the notification contains a request to enter into an obligation to desist from infringement, to state to what extent the proposed obligation to desist from infringement goes beyond the infringement notified.

A notification which does not meet the conditions set out in the first sentence shall not be effective.

(3) Where the notification is rightful and meets the conditions set out in subsection (2), first sentence, numbers 1 to 4, reimbursement of expenses necessarily incurred may be demanded. Where the services of a lawyer have been used, the reimbursement of expenses necessarily incurred shall be limited as regards statutory fees to fees in accordance with a value of the object of the claim to desist and the claim for removal of 1,000 euros if the person notified

1. is a natural person who does not use the works protected under this Act or other subject-matters protected under this Act for his commercial or self-employed business activity, and

2. is not already obliged to desist from infringement on the basis of a claim of the notifying party by contract, a legally binding decision or a temporary injunction.

The value referred to in the second sentence shall also be decisive where a claim to desist and a claim for removal are asserted in parallel. The second sentence shall not apply where the value referred to is unreasonable based on the specific circumstances of the individual case.

(4) Where the notification is without entitlement or ineffective, the person notified may demand reimbursement of the necessary expenses incurred in respect of defending his rights, unless the person giving notification was not able to recognise at the point in time when notification was made that the notification was without entitlement. Rights to reimbursement over and above this shall remain unaffected.

b) Administrative.

Nothing to report.

c) Criminal.

See above, question 1. In practice, these provisions are not relevant. In particular, to require relevant personal information it is not necessary to start criminal proceedings, since there are private claims available (see *infra*, question 10).

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law against intermediaries to address online copyright infringement by third party users of their services?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

Remedies against intermediaries:

- Injunctions according to Section 1004 German Civil Code against “interferers” (= “Störer”)

Any person who has willfully made a causal contribution to the direct copyright infringement by a third party (e.g. running an online platform) can be held liable for injunctive relief if the contributor has violated a reasonable duty of care to prevent such direct infringements. Typically, a reasonable duty of care to prevent such direct infringements consists of deleting the content of third parties upon notification (“notice-and-take-down”). Additionally, the “interferer” (“Störer”) has to take reasonable measures, such as filtering, to prevent further comparable infringements in the future (“notice-and-action”) (BGH, 12.7.2012 – I ZR 18/11 para 29, 32 – Alone in the dark).

- Damages are not available.
- Furthermore, there are obligations to inform about the direct infringer according to Section 101 *Act on Copyright and related rights*

Section 101: Right of information

(1) Any person who infringes copyright or another right protected under this Act on a commercial scale may be required by the injured party to provide information without delay as to the origin and the distribution networks of infringing copies or other products. The commercial scale may be deemed to exist on the basis either of the number of infringements or the severity of the infringement.

(2) In cases of manifest infringement or in cases where the injured party has brought a court action against the infringer, such a right shall exist, without prejudice to subsection (1), also against any person who, on a commercial scale,

1. was in possession of infringing copies,

2. was using infringing services,

3. was providing services used in infringing activities, or

4. was indicated by the person referred to in number 1, 2 or 3, as being involved in the production, manufacture or distribution of such copies, other products or services,

unless the person concerned would, under sections 383 to 385 of the Code of Civil Procedure, be entitled to refuse testimony as a witness in the proceedings against the infringer. In the event of a claim pursuant to the first sentence being brought before a court, the court may, upon application, suspend the litigation pending against the infringer until disposal of any litigation being conducted in respect of a right to information. The person obliged to provide information may demand reimbursement from the injured party of the expenses necessarily incurred in providing the information.

(3) The person obliged to provide information must supply the following information:

1. The name and address of the producers, suppliers and other previous holders of the copies or other products, the users of the services, as well as the intended wholesalers and retailers, and

2. the quantities of produced, delivered, received or ordered copies or other products, as well as the prices paid for the copies or other products in question.

(4) The claims under subsections (1) and (2) shall be precluded where their assertion is disproportionate in the individual case.

(5) Where the person obliged to provide information intentionally or gross negligently provides incorrect or incomplete information, he shall be obliged to reimburse the injured party for the resulting damage.

(6) Any person who provides truthful information without having been obliged to do so according to subsection (1) or (2) shall only be held liable against third parties if he knew that he was not obliged to provide the information.

(7) In the event of an obvious infringement, the obligation to provide information may be issued by way of a temporary injunction according to sections 935 to 945 of the Code of Civil Procedure.

(8) The findings may be used in criminal proceedings or in proceedings based on the Act on Regulatory Offences in respect of an act committed before the information was provided against the person obliged to provide information or against a relative designated in section 52 (1) of the Code of Criminal Procedure only with the consent of the person obliged to provide information.

(9) Where the information can be provided only by using traffic data (section 3, number 30, of the Telecommunications Act), a prior judicial order, which must be applied for by the injured party as to the admissibility of use of the traffic data shall be required for the provision of such information. Sole jurisdiction for issuing any such order shall lie, regardless of the value of the claim, with the regional court in whose district the person obliged to provide information has his

domicile, his seat or a branch office. The decision shall be rendered by the civil division. The provisions of the Act on Proceedings in Family Matters and in Matters of Non-Contentious Jurisdiction shall apply mutatis mutandis to the proceedings. The costs of the judicial order shall be borne by the injured party. The remedy of immediate complaint is admissible in respect of the regional court decision. It shall be submitted within a period of two weeks. The provisions on the protection of personal data shall otherwise remain unaffected.

(10) The fundamental right to secrecy of telecommunications (Article 10 of the Basic Law) shall be limited on account of subsection (2) read in conjunction with subsection (9).

There are no differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

b) Administrative.

Nothing to report.

c) Criminal.

Nothing to report.

9. To the best of your knowledge, are there significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

Nothing to report.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

Yes they have. As mentioned above there is an obligation to disclose personal data of individuals involved in copyright infringing activities according to Section 101 (2) No. 3, (3), (9) *Act on Copyright and Related Rights*.

a) If yes, what conditions must be met for that obligation to arise?

In order to obtain information about the direct infringer from a person e.g. an access-provider, who was providing services used in infringing activities two conditions must be met:

(1) First, a manifest infringement has to be established (Section 101 (2) Nr. 3 *Act on Copyright and Related Rights*). In practice, if an IP-address was identified within filesharing activities this condition is met.

(2) Secondly, a court order is necessary (Section 101 (9) *Act on Copyright and Related Rights*)

b) If yes, what type of personal data is typically requested?

The kind of data to be requested is administered by Section 101 (3) No. 1 *Act on Copyright and Related Rights*. Accordingly, the (1) name and (2) the physical address can be requested.

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

Holders of copyrights and holders of related rights can apply for remedies, sanctions and procedures as mentioned above.

Additionally, those who have an exclusive license can apply for remedies, sanctions and procedures mentioned above. This applies to collecting societies (CMO) as well. It also would be true for professional defense bodies.

Licensees, who do not have an exclusive license but a non-exclusive license are not entitled to start legal proceedings.

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

The most widely used and most effective enforcement measure are “cease-and-desist”-letters. To prevent an injunction granted by a court the infringer has to enter into an obligation to desist from infringements accompanied by an equitable contractual penalty. This is a private enforcement measure.

- Please indicate whether the measures refer to public or private enforcement.

a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?

No.

b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.

Nothing to report.

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

Recently, free wifi has been discussed in parliament. To protect copyrights and related rights, everybody who runs a local wireless area network is obliged to secure the network by means of a password in order to prevent copyright infringements. Since access to Internet is considered as basic infrastructure this is highly controversial.

Secondly, the practice of sending “cease-and-desist”-letters has been a contentious point. The fees to be borne by infringers are considered too high. Furthermore, quite often non-infringers are notified. Fees requested are not justified in these cases.

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions/campaigns aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

Well-known is a campaign against copyright infringement funded by the cinema and lending industry.

- (<http://www.hartabergerecht.de/spiel-regeln.html>). Commercials (e.g. <https://www.youtube.com/watch?v=U6H4iv1iOOU>) have been broadcasted in cinemas. The campaign started in 2005 and aimed at copyright infringing activities in general.
- See also <http://www.respectcopyrights.de/>

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

As mentioned above, notifications (“Abmahnungen”) and “cease-and-desist”-letters are a widespread remedy to combat copyright infringements in Germany.

In 2015 the German Federal Court held for the first time that blocking injunctions could be available (BGH, 26.11.2015 – I ZR 174/14 – Störerhaftung des Access-Providers)

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

Nothing to report.

Questionnaire the Netherlands

STEF VAN GOMPEL, Senior researcher and Lecturer, University of Amsterdam, Institute for Information Law

Last updated: 1 June 2018

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded **red**.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.

The following legal instruments regulate online copyright infringement in the Netherlands:

- *Auteurswet*: Copyright Act
- *Wet op de naburige rechten*: Neighboring Rights Act
- *Burgerlijk Wetboek & Wetboek van Burgerlijke Rechtsvordering*: Civil Code & Code on Civil Procedure
- *Wetboek van Strafrecht & Wetboek van Strafvordering*: Criminal Code & Code of Criminal Procedure

2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?

Dutch law does not define the notion of ‘intermediary’ specifically for copyright purposes. Article 3:15d(3) of the Civil Code provides the following general definition of a ‘service of the information society,’ which is understood as “any service which is usually performed in exchange for a financial consideration, at or from a distance by electronic transmission, at the individual request of the consumer of the service without parties having been simultaneously present at the same place. A service is performed electronically if it is sent out, transmitted and received exclusively by wire, by radio or by means of optical or other electromagnetic resources, using electronic equipment for the processing, including digital compression, and the storage of data.”

3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
- Depends on the commercial or for-profit nature or intent of the use or user;
- Is uncertain and, if so, why;
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

Unless explicitly specified, the infringing nature of the below acts does not depend on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content; does not depend on the commercial or for-profit nature or intent of the use or user; and does not vary depending on the type of protected content (music, audio-visual, books, and video games).

a) Downloading copyright-protected content from illegal/unauthorized sources on the Internet.

Yes. Up until the CJEU's decision of 10 April 2014 in the *ACI Adam* case (C-435/12), downloading copyright-protected content from illegal/unauthorized sources was considered to be covered by the private copying exception of article 16c of the Copyright Act (*Kamerstukken II* 2002/03, 28 482, nr. 5, p. 32-33; *Rechtbank Haarlem* 12 May 2004, ECLI:NL:RBHAA:2004:AO9318, *Techno Design/Stichting Brein*, at 6.18), with the exception of computer programs (including video games) to which the private copying exception does not apply (article 45n of the Copyright Act).

The CJEU, however, held that article 5(2)(b) of Directive 2001/29 does not permit Member States to adopt legislation that also allows reproductions for private use to be made from an unlawful source (CJEU 10 April 2014, case C-435/12, ECLI:EU:C:2014:254, *ACI Adam*).

According to the Dutch government, article 16c of the Copyright Act necessitated no amendment as a result of the *ACI Adam* decision, since the CJEU's decision is binding upon the EU Member States and has immediate effect in the Netherlands (*Kamerstukken II* 2013/14, 29 838, nr. 72, p. 3). As of 10 April 2014, therefore, downloading copyright-protected content from illegal/unauthorized sources on the Internet also qualifies as an act of copyright infringement in the Netherlands.

b) Streaming copyright-protected content from illegal/unauthorized sources on the Internet.

Yes, at least in the context of streaming content on Kodi boxes or similar media players. On 26 April 2017, the CJEU ruled that the streaming of protected videos from an illegal website does not, as its sole purpose, enable a lawful use in the meaning of article 5(1) of Directive 2001/29 to be made of such works (CJEU 26 April 2017, case C-527/15, ECLI:EU:C:2017:300, *Stichting Brein/Wullems*). The CJEU held that to be lawful, a use must either be authorised by the right holder (which was not the case) or not be restricted by the applicable law (which was not the case either). In the particular circumstances of the case, the streaming took place on media players that were advertised with the deliberate intent of facilitating the streaming from illegal/unauthorized sources. In view of this, the CJEU found that it was 'deliberately and in full knowledge of the circumstances that the purchaser of such a player accesses a free and unauthorised offer of protected works'. Knowledge of the illegal nature of the source by the purchasers of the media player thus formed an indication for the CJEU that streaming on such a media player cannot have a lawful use of works as its sole purpose.

c) Stream-ripping copyright-protected content.

Uncertain. There is no case law on this matter. Given that stream-ripping is functionally equivalent to downloading, it might be expected that it be treated the same way as downloading copyright-protected content. This would mean that stream-ripping from illegal/unauthorized sources would be a copyright infringement, whereas stream-ripping from legal/authorized sources would be permitted by the private copying exception. In the absence of case law, however, this cannot be stated with certainty. Under Dutch law, certain types of stream-ripping could possibly also constitute a prohibited circumvention of technological measures within the meaning of article 29a of the Copyright Act, but – here too – there is no case law to support this claim and hence cannot be stated with certainty.

d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.

Yes. Uploading copyright-protected content to a website or online platform accessible to the public is an act of communication/disclosure to the public (*openbaarmaking*) within the meaning of article 12 of the Copyright Act. It therefore qualifies as an act of copyright infringement if the uploading occurs without the authorization of the rights holder.

e) Posting **hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.**

- *Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard **surface hyperlink**, **deep-link**, **embedded or framing hyperlink**).*

Yes. On 8 September 2016, the CJEU ruled that a hyperlinker intervening ‘in full knowledge of the consequences of his conduct in order to give customers access to a work illegally posted on the internet’ makes a communication to the public of that work: such intervention reaches a new public, since the rights holder did not consent to making the work freely available on the other website (CJEU 8 September 2016, case C-160/15, ECLI:EU:C:2016:644, *GS Media/Sanoma*). The CJEU argued that a not-for-profit hyperlinker cannot be assumed to have such knowledge, unless ‘it is established that such a person knew or ought to have known that the hyperlink he posted provides access to a work illegally placed on the internet’, e.g., if he was notified thereof by the copyright holder. A for-profit hyperlinker, on the other hand, must be presumed to have full knowledge, because such a person can be expected to carry out ‘the necessary checks to ensure that the work concerned is not illegally published on the website to which those hyperlinks lead.’ This presumption is rebuttable. ^[1]_{SEP}

It does not matter which type of hyperlinking technique is applied, e.g. standard surface linking, deep linking, embedded or framed linking (CJEU 13 February 2014, case C-466/12, ECLI:EU:C:2014:76, *Svensson/Retriever*). Arguably, the hyperlink posted must be a clickable link. Whether the case law of the CJEU also applies to non-clickable hyperlinks, such as framed links that directly show the work as is without the need to click on the link, is yet unresolved and therefore still uncertain.

f) The sale of **Kodi boxes or similar devices.**

Yes. On 26 April 2017, the CJEU decided that the sale of media players with preinstalled add-ons that provide links to illegal video streams constitutes a communication to the public (CJEU 26 April 2017, case C-527/15, ECLI:EU:C:2017:300, *Stichting Brein/Wullems*). The CJEU held that the vendor, with full knowledge of the consequences of its conduct, gave purchasers of the media player direct access to protected works. The sale of the media player thus constituted a communication of works and not a mere provision of physical facilities: without the add-ons, it would be more difficult to benefit from the works to which the add-ons link. The communication also reached a public, since it was directed at an indeterminate and fairly large number of potential purchasers with an Internet connection, and also a new public, since advertisements revealed that the vendor of the media player, who operated for profit, had full knowledge of the fact that the preinstalled add-ons with hyperlinks gave access to works published illegally on the Internet. Stichting Brein reported that, in the first half of 2017, it has

stopped the sale of illegal media players of 154 vendors in the Netherlands (see the press release of Stichting Brein of 20 July 2017: <<https://stichtingbrein.nl/nieuws.php?id=465>>).

g) Other types of unauthorized online use of copyright-protected content not listed above.

Nothing specific to report for the Netherlands.

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

Dutch law does not differentiate between acts of copyright infringement by children and by adults as such, but parents or guardians (persons who exercise parental responsibility or legal guardianship over a child) may be held liable for copyright infringing acts of children in the following cases:

- A copyright infringing act of a child who has not yet reached the age of fourteen years: such act cannot be attributed to him as a tortious act (article 6:164 of the Civil Code), but parents or guardians are liable for damage caused to a third person by this act, provided that it could have been regarded as a tortious act of that child if its age would not have stand in the way (article 6:169(1) of the Civil Code).
- A copyright infringing act of a child who has reached the age of fourteen years, but not yet the age of sixteen years: parents or guardians are liable for damage caused to a third person by this child's fault, unless they cannot be blamed for not preventing this child's behavior (article 6:169(2) of the Civil Code); the child himself can also be (partially) liable for damage caused to a third person by this act, provided that it can be regarded as a tortious act.
- A copyright infringing act of a child of sixteen years and older: the child is liable for damage caused to a third person by this act, provided that it can be regarded as a tortious act.

In one case concerning a fifteen-year-old boy who managed and ran the website www.soccer4u.nl on which he published two photos of Johan Crujff without authorization and without attribution of the photographer, the court held the boy liable to pay damages of €2.420 plus interest and bear the legal costs of €1.647,93 (Rechtbank 's-Hertogenbosch, 2 October 2008, ECLI:NL:RBSHE:2008:BF9979). The court did not hold the parents liable pursuant to article 6:169(2) of the Civil Code, as the parents could not be blamed for not preventing the boy's infringing act. The court considered it normal that a fifteen-year-old boy is running a website on soccer without parental control. The court also found that the parents were under no duty to specifically monitor their son's behavior in exploiting the website (Rechtbank 's-Hertogenbosch, 3 September 2009, ECLI:NL:RBSHE:2009:BJ7462).

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country's law? If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.

Article 6:196c of the Civil Code contains safe-harbor provisions exempting 'providers of information society services' (see Q3 above), under specific circumstances, from civil liability for acts conducted by third parties using their services. Distinguishing between mere conduit (sections 1 and 2), caching (section 3), and hosting (section 4) activities, the provision provides the following:

"1. A person who provides a service of the information society as meant in article 3:15d, paragraph 3, of the Civil Code, consisting of the transmission in a communication network of information provided by a recipient of the service or providing access to a communication network, is not liable for the information transmitted, on condition that the provider:

- a. does not initiate the transmission;
- b. is not the one who decides to whom the information will be transmitted; and
- c. has not selected or modified the information contained in the transmission.

2. For the purpose of paragraph 1 the acts of transmission and of merely providing access to a communication network include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. A person who provides a service of the information society as meant in article 3:15d, paragraph 3, of the Civil Code, consisting of the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, is not liable for the automatic, intermediate and temporary storage of that information, on condition that the provider:

- a. does not modify the information;
- b. complies with conditions on access to the information;
- c. complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
- d. does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and;
- e. acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

4. A person who provides a service of the information society as meant in article 3:15d, paragraph 3, of the Civil Code, consisting of the storage of information provided by a recipient of the service, is not liable for the information that is stored at the request of a recipient of the service, on condition that the provider:

- a. does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or;
- b. upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

5. The above mentioned paragraphs do not affect the possibility to get a court order to terminate or prevent an infringement or an injunction for the removal or disabling of access to information.”

Article 54a of the Criminal Code exempts providers of telecommunications services from criminal prosecution in a manner comparable to the safe-harbors of article 6:196c of the Civil Code:

“An intermediary that provides a telecommunications service consisting of the transfer or storage of data originating from others, will not be prosecuted in connection with these activities as long as he complies with an order by a public prosecutor, after written authorization by the examining judge on request of the public prosecutor, to take all reasonable measures to prevent access to the data under investigation.”

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

Dutch law does not give reason for any further legal uncertainty beyond the uncertainty that has arisen as a result of the case law of the CJEU on the right of communication to the public. That right is now interpreted so broadly that also the making available and management of online file sharing platforms, such as the Pirate Bay, is regarded as constituting a communication to the public (CJEU 14 June 2017, case C-610/15, ECLI:EU:C:2017:456, *Stichting Brein/Ziggo*). For online hosting platforms, especially the ones with a hybrid character, this raises uncertainty about when they can benefit from safe harbor protection and when their activities are considered to be a communication to the public.

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:

- The suspension from the Internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.
- The monitoring or **filtering** of content.
- The **blocking** and removing of infringing content, including notice-and-takedown.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- **Graduated response systems.**

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

The Netherlands makes no distinction in enforcement measures, procedures, remedies, and sanctions between different types of protected content (music, audio-visual, books, and video games).

a) Civil.

A copyright holder can initiate the following civil proceedings against online copyright infringement by users: substantive proceedings, preliminary relief proceedings or ex parte proceedings.

In an ex parte proceeding, the court in preliminary relief proceedings may grant a preliminary ex parte injunction against the alleged infringer of an intellectual property right in urgent cases, in which delay would cause irreparable damage to the rights holder; an ex parte injunction is rendered upon a request made through a petition, without having to summon the alleged infringer; the decision is immediate provisionally enforceable (article 1019e Code of Civil Procedure). Except for preliminary injunctions, no remedies and no recovery of costs are available in an ex parte proceeding.

In substantive proceedings and preliminary relief proceedings, the following remedies are available to address online copyright infringement by users (note that in the case of preliminary relief proceedings, a separate urgent interest is required for claiming damages and ancillary claims):

- injunctions to stop the infringement;
- monetary damages;

- in addition to damages: the surrender of profits accrued by reason of the infringement, including the rendering account thereof (article 27a Copyright Act);
- claiming of monies that may be assumed to have been obtained by or as a result of an infringement of the copyright (article 28(2)(b) Copyright Act);
- an order against the person who has infringed his rights to inform the rights holder of everything he knows about the origin and distribution channels of the infringing goods or services and to provide him with all the relevant information (article 28(9) Copyright Act);
- an order to have appropriate measures taken for the dissemination of information about the decision at the expense of the person who has infringed the copyright (article 28(10) Copyright Act); and
- full cost recovery of reasonably made attorney's expenses (article 1019h Code of Civil Procedure).

b) Administrative.

N/A

c) Criminal.

Pursuant to article 31 Copyright Act, anyone who intentionally infringes another person's copyright is punishable with imprisonment for not more than six months or with a fine of the fourth category (max. €16.750; as of 1 January 2016: €20.5 thousand). This requires (criminal) intent and proof of actual copyright infringement by the suspect.

Punishable with imprisonment for a term of not more than one year or with a fine of the fifth category (max. €67 thousand; as of 1 January 2016: €82 thousand) is anyone who intentionally: (a) publicly offers for distribution; (b) has on hand, for the purpose of reproduction or distribution; (c) imports, conveys in transit or exports; or (d) keeps in pursuit of profit; an object that comprises a work infringing another person's copyright (article 31a Copyright Act). This also requires (criminal) intent, but the burden of proof is lower: no proof is needed of actual copyright infringement by the suspect, but only that the suspect actually committed one of the given acts that give rise to copyright infringement.

Criminal sanctions under articles 31 and 31a Copyright Act are elevated to imprisonment for a term of not more than four years or a fine of the fifth category (max. €67 thousand; as of 1 January 2016: €82 thousand) if the crimes are committed by a person who makes it his profession or business to commit the crimes referred to in those provisions (article 31b Copyright Act).

Pursuant to article 31 Copyright Act, anyone who commits the acts listed in article 31a Copyright Act with respect to an object which he can reasonably presume comprises a work that infringes another person's copyright, is punishable with a fine of the third category (max. €6.7 thousand; as of 1 January 2016: €8.2 thousand). This does not require (criminal) intent, but is a culpable infringement.

Article 32a Copyright Act states that anyone who intentionally: (a) publicly offers for distribution; (b) has on hand, for the purpose of reproduction or distribution; (c) imports, conveys in transit or exports; or (d) keeps in pursuit of profit; any means the sole intended purpose of which is to facilitate the removal or circumvention of any technological measure applied to protect a work, without the consent of the author or his successor in title, is punishable with imprisonment for a term of not more than six months or with a fine of the fourth category (max. €16.750; as of 1 January 2016: €20.5 thousand).

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law against intermediaries to address online copyright infringement by third party users of their services?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

Notice-and-takedown: the Netherlands has no statutory notice-and-takedown procedure. On the basis of article 6:196c of the Civil Code, however, intermediaries can be ordered to implement effective notice-and-takedown procedures (Hof Amsterdam 19 August 2014, ECLI:NL:GHAMS:2014:3435, *NSE/Brein*). In practice, several Dutch intermediaries have adopted voluntary notice-and-takedown procedures at their own initiative to benefit from safe harbor protection for hosting and caching activities under Article 6:196c of the Civil Code. Together with the government and interest groups, they have established a Code of Conduct on Notice-and-Take-Down setting out how intermediaries are expected to respond to requests for removing content, including copyright infringing content (see *Gedragscode Notice-and-Take-Down*, available at: <<https://ecp.nl/publicaties/ntd-gedragscode-nl/>>).

Blocking access to websites: Article 26d Copyright Act provides that, upon application by the author, the court may order an intermediary whose services are used by a third party to infringe copyright, to cease and desist from providing the services that are used for that infringement. This provision forms the basis for courts to issue orders to block the domain names and IP addresses of infringing websites. In 2014, the Court of Appeals of The Hague ruled that the practice of blocking access to the online sharing platform ‘The Pirate Bay’ was ineffective and therefore discontinued the blocking order that was issued by the first instance court (Hof Den Haag 28 January 2014, ECLI:NL:GHDHA:2014:88, *Ziggo/Brein*, par. 5.24-5.26). In 2015, in keeping with the CJEU’s judgment in *UPC Telekabel Wien* (CJEU 27 March 2014, case C-314/12, ECLI:EU:C:2014:192), the Supreme Court held that the Court of Appeals had applied too stringent criteria to test the effectivity of the website blocking order (Hoge Raad 13 November 2015, ECLI:NL:HR:2015:3307, *Brein/Ziggo*, par. 4.4.2).

Measures for identification of the infringer: Pursuant to article 28(9) Copyright Act, the court, upon application by the rights holder, can issue an order against a third party who is providing services used in the infringing activities on a commercial scale or who has been indicated by one of the said third parties as being involved in the provision of these services to inform the rights holder of everything he knows about the origin and distribution channels of the infringing goods or services and to provide him with all the relevant information about the infringement. This third party may refuse to provide information that could serve as evidence of his or his next of kin’s (the persons referred to in article 165(3) Code of Civil Procedure) participation in an infringement of copyright (see also Q10 below).

No general filtering obligation: In line with article 15(1) E-Commerce Directive, the Netherlands does not impose a general duty on intermediaries to monitor the content which they transmit or store or to actively seek circumstances or facts indicating illegal activity on their platforms.

b) Administrative.

N/A

c) Criminal.

The Dutch Copyright Act does not contain criminal provisions that are specifically targeted at (online) intermediaries. To the extent that intermediaries commit, or are involved in, any of the crimes referred to in articles 31, 31a, 31b, 32 and 32a Copyright Act, they are punishable under criminal law in the same ways as mentioned above under Q7(c).

- 9. To the best of your knowledge, are there significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.**

No.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

Intermediaries can be obliged to disclose personal data of individuals involved in copyright infringing activities to rights holders on the basis of article 28(9) Copyright Act, which is an implementation of article 8(1) of Directive 2004/48 (*compare* CJEU 16 July 2015, case C-580/13, ECLI:EU:C:2015:485, *Coty Germany/Stadtparkasse*, holding that this provision not only relates to proceedings concerning an infringement of an intellectual property right, but also covers requests for information made in the context of proceedings relating to an obvious infringement of intellectual property rights).

In addition, in the *Lycos/Pessers* case, the Supreme Court held that online intermediaries may also be obliged to disclose personal data of individuals involved in copyright infringing activities to rights holders on the basis of a general duty of care resulting from article 6:162 Civil Code. This is the case if (i) there is substantial likelihood that the content is unlawful and could cause harm to the rights holder; (ii) the rights holder has a reasonable interest in obtaining the personal data; (iii) it is plausible that in the specific case there is no less radical possibility to obtain the personal data; and (iv) the interests of the rights holder outweigh the interests of the intermediary and the person whose data is requested (Hoge Raad 25 November 2005, ECLI:NL:HR:2005:AU4019, *Lycos/Pessers*).

a) If yes, what conditions must be met for that obligation to arise?

Pursuant to article 28(9) Copyright Act, it requires a court order to oblige intermediaries to disclose personal data of individuals involved in copyright infringing activities to rights holders. However, on the basis of the general duty of care as formulated in the *Lycos/Pessers* case, intermediaries may also be compelled to make their own independent assessment and hand over personal data to rights holders without a court order. After all, if intermediaries fail to disclose personal data under the conditions spelled out in that case, they may be acting unlawfully for not complying with the general duty of care imposed on them (Hoge Raad 25 November 2005, *Lycos/Pessers*, par. 5.3.4).

Interestingly, in 2015, the court of first instance of The Hague required Google to inform an alleged copyright infringer of the request by Brein to disclose his personal data, so as to permit this person to oppose to the request, and to actually release the data to Brein if the request was not challenged within two weeks (Rechtbank Den Haag 5 October 2015, ECLI:NL:RBDHA:2015:11408, *Brein/Google*).

b) If yes, what type of personal data is typically requested?

Depending on the case, what is typically requested are IP addresses that have been used for infringing copyright, account information (names and email addresses used), NAW data (name, address, place of residence) of subscribers and sometimes payment details.

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

Civil action: The author or his successor in title can enforce copyright. Where two or more persons hold the joint copyright in one and the same work, any one of them may enforce the right, unless otherwise agreed (Article 26 Copyright Act). Notwithstanding the assignment of his copyright in whole or in part, the author retains the right to bring an action for compensation against the person who has infringed the copyright; after the author's death, this right vests in the author's heirs or legatees until the copyright expires (Article 27 Copyright Act). Copyright can also be enforced by licensees or organizations such as Stichting Brein or collective rights management organizations, but only if they have obtained the right to do so from the author or his successor in title.

Criminal action: Only the public prosecutor can start a criminal prosecution. Just like everyone who is aware of unlawful acts that have taken place, rights holders are authorized to report infringements of copyright to the police (article 161 Code of Criminal Procedure). Criminal investigations are carried out by the Piracy Investigations Team of the FIOD (Fiscal Information and Investigation Service), operating the supervision of a special unit of the Public Prosecution Service. In the Netherlands, the Public Prosecution Service does not have copyright infringement high on its priority list.

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

- Please indicate whether the measures refer to public or private enforcement.

One of the most widely used enforcement measure in the Netherlands is the issuing of court orders to require Internet access providers to block access to infringing websites. Most of these orders have been initiated by *Stichting Brein*, a private enforcement agency that represents large Dutch content industries. In practice, as noted under Q8(a), it is also common for Dutch intermediaries to employ voluntary notice-and-takedown procedures. *Stichting Brein* further initiates civil enforcement action against large-scale infringers if their identity can be obtained and, where appropriate, reports specific cases to the public prosecutor as criminal cases. Criminal proceedings against copyright infringers in the Netherlands do not often take place, however.

a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?

No.

b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.

In several cases, Dutch Internet access providers have been summoned by the courts to block their subscribers' access to infringing websites. Probably the most high profile case is the case of *Stichting Brein* (a private enforcement agency) against *Ziggo* and *XS4ALL* (Dutch internet access providers) in respect of the blocking of subscribers' access to *The Pirate Bay* (Hof Den Haag 28 January 2014, ECLI:NL:GHDHA:2014:88, *Ziggo & XS4ALL/Stichting Brein*). This case is currently pending at the Dutch Supreme Court (Hoge Raad), which has to answer the case in accordance with the ruling of the CJEU of 14 June 2017 (case C-610/15, ECLI:EU:C:2017:456, *Stichting Brein/Ziggo*). Interestingly, on 22 September 2017, the Preliminary Relief Judge of the District Court of The Hague already issued, in anticipation of the judgment of the Supreme Court, a provisional order to block access to *The Pirate Bay* for subscribers of *Ziggo* and *XS4ALL* (Vzr. Rechtbank Den Haag 22 September 2017, ECLI:NL:RBDHA:2017:10789, *Stichting Brein/Ziggo & XS4ALL*). On 12 January 2018, other internet service providers in the Netherlands were summoned to do the same (Vzr. Rechtbank Midden-Nederland 12 January 2018, ECLI:NL:RBMNE:2018:114, *Stichting Brein/KPN, T-mobile, Tele2, Zeelandnet & CAIW*). On 16 March 2018, A-G Van Peursem advised the Dutch Supreme Court to annul the judgment of the Court of Appeals of The Hague of 28 January 2014 and to refer the case to another Court of Appeals for a fresh examination in light of the CJEU jurisprudence (Conclusie AG HR 16 March 2018, ECLI:NL:PHR:2018:202, *Stichting Brein/Ziggo & XS4ALL*).

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

Except for the general topic of what are effective, appropriate means of enforcing copyrights that take full account of the balance between different interests and fundamental rights of all concerned (rights holders, intermediaries and users), there are some discussions in the Netherlands whether, in addition to private enforcement by rights holders, there is also a task for the State to enforce copyright online (public enforcement). Especially film producers are vocal in this debate. The State maintains however that enforcement of copyright is principally the responsibility of the rights holders concerned.

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions/campaigns aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

In the Netherlands, several (informational) websites on copyright have been launched by *Stichting Federatie Auteursrechtbelangen*, a cooperation of organizations representing creators, performing artists, producers and publishers. One of those is <https://www.thecontentmap.nl/>, launched in January 2014 with the aim of guiding the public to legal content (audiovisual works, music, games, ebooks, images) available online. The website is meant to promote the use of legal content and prevent that people use illegal channels to get access to copyright protected works. Other, more general initiatives, are the websites <https://www.auteursrecht.nl/> (providing information on copyright for the general public) and <http://auteursrechtvoorjou.nl/> (doing the same but specifically for children).

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

No.

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

Poort, J., Weda, J. (2015). Elvis Is Returning to the Building: Understanding a Decline in Unauthorized File Sharing. *Journal of Media Economics*, 28(2), pp. 63-83.

Leenheer, J., Poort, J. (2014). “Alleen maar nette mensen”: Consumentenonderzoek Downloadgedrag Films. CentERdata/IViR, Tilburg/Amsterdam.

Poort, J. Leenheer, J. (2012). *File sharing 2012*. Downloading from illegal sources in the Netherlands. IViR/CentERdata, Amsterdam/Tilburg.

Eijk, N. van, Poort, J. & Rutten, P. (2010). Legal, Economic and Cultural Aspects of File Sharing. *Communications & Strategies*, 77, (1st Q. 2010), 35-54.

A. Huygen, P. Rutten, S. Huveneers, S. Limonard (TNO), J. Poort, J. Leenheer, K. S. Janssen (SEO Economic Research), N. van Eijk, N. Helberger (IViR), *Ups and downs. Economic and cultural effects of file sharing on music, film and games*, Delft/Amsterdam, February 2009, Commissioned by: Ministries van Education, Culture and Science, Economic Affairs and Justice. TNO-rapport 34782, SEO-report 2009-2A. (Translation of SEO-report 2009-2)

Questionnaire Poland

TOMASZ TARGOSZ, Institute of Intellectual Property Law, Jagiellonian University Kraków

Last updated: 2 June 2018

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded **red**.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.

The relevant legal instruments are the Copyright Act (arts 79 and 80), the E-Commerce Act (arts 12 to 15), the Civil Code (arts 422 and 439), and the Criminal Code.

Relevant provisions for criminal are found in the Copyright Act (arts 115 to 118) and the Criminal Code (arts 278 and 299).

- **Arts 79 and 80 Copyright Act (The Act on Copyright and Related Rights)**

Art. 79

1. The rightholder may request from the person who infringed his/ her author's economic rights to:

- 1) cease the infringement;*
- 2) eliminate the consequences of the infringement;*
- 3) repair the inflicted damage:*

a) on the general terms or

b) [by virtue of the judgment of the Constitutional Tribunal of 23 July 2015, docket No. SK 32/14 (Dziennik Ustaw 2015, item 932), this letter, within the scope in which the rightholder, whose author's economic rights have been infringed, may request that the person who has violated those rights repair the inflicted damage by payment of the sum of money in an amount corresponding to, where the infringement is culpable, triple amount of respective remuneration that would have been due as of the time of claiming it in exchange for the rightholder's consent for the use of the work, was found to be in breach of Article 64, paragraphs 1 and 2, read in conjunction with Article 31, paragraph 3 and in conjunction with Article 2 of the Constitution of the Republic of Poland] by payment of double or, where the infringement is culpable, triple the amount of respective remuneration that would have been due as of the time of claiming it in exchange for the rightholder's consent for the use of the work;

4) render the acquired benefits.

2. Irrespective of the claims referred to in paragraph 1, the rightholder may demand a single or multiple announcements of a press declaration having the proper wording and form, or communicating to the public all or a part of a court pronouncement issued in the examined case, in the manner and within the scope defined by the court Irrespective of the claims specified in paragraph 1, the rightholder may demand:

1) a single or multiple announcements of a press declaration having the proper wording and form, or communicating to the public all or a part of a court pronouncement issued in the examined case, in the manner and within the scope defined by the court;

2) payment by the person who breached the author's economic rights of an appropriate sum of at least double the probable value of the benefits received by the perpetrator of the infringement in favour of the Fund referred to in Article 111, provided that the infringement was culpable and has been committed within the scope of economic activity performed by the perpetrator in the name of a third party or in his own name even if on account of a third party.

3. A person who breached the author's economic rights may be instructed by the court, at such person's request and with the rightholder's consent, if the breach is non-culpable, to pay a relevant sum to the rightholder if discontinuance of the breach or elimination of the consequences of the breach would have been excessively onerous for the perpetrator.

4. When issuing its decision on breach of law the court may adjudge, at the rightholder's request, on illegally produced objects and means and materials used to produce them and in particular, the court may adjudge on their withdrawal from trading, on assigning them to the rightholder as part of damages or on their destruction. While issuing its decision the court shall take into account the weight of the breach and third party interests.

5. It shall be presumed that the means and materials referred to in paragraph 4 are owned by the person who breached the author's economic rights.

6. The provision of paragraph 1 shall respectively apply to elimination or circumvention of technological protective measures which prevent any access to, reproduction or dissemination of a work, provided that the objective of such acts is illegal use of such work.

7. Paragraphs 1 and 2 shall apply respectively in the event of unauthorised removal or change of any electronic information on the administration of copyright or neighbouring rights, as well as intentional dissemination of works with such information having been illegally removed or modified.

Art. 80

1. The court competent to hear the cases of infringement of the author's economic rights in the locality where the perpetrator conducts its activity or where his property is located, also prior to filing suit, shall consider, within no more than 3 days of filing, an application of a party with legal interest therein:

1) for securing evidence and securing claims related thereto;

2) for obliging the person who infringed the author's economic rights to provide information and any documentation specified by the court and being material to the claims referred to in Article 79, paragraph 1;

3) for obliging a person other than the infringing party to provide information material to the claims defined in Article 79, paragraph 1 on the origin, distribution networks, volume and price of goods or services which infringe the author's economic rights, provided that:

a) such person has been confirmed to have goods which breach the author's economic rights; or

b) such person has been confirmed to benefit from services which breach the author's economic rights; or

c) such person has been confirmed to render services used in any acts which the breach author's economic rights; or

d) the person specified in letters a, b or c indicated a person who participated in production, manufacturing or distribution of goods or rendering of services in breach of the author's economic rights and the purpose of any of the above actions is to generate, directly or indirectly, profit or any other economic benefit, although it does not include any actions by consumers acting in good faith.

2. If it admits any evidence or considers any applications referred to in paragraph 1, the court ensures that the entrepreneur's business secrets as well as all other secrets protected by statutory law are kept confidential.

3. *The duty referred to in paragraph 1, subparagraphs 2 and 3 may be avoided exclusively by anyone who under the Code of Civil Procedure could have refused to give testimony or to respond to any questions asked of him acting as witness.*
4. *If justified, the court may condition the issuance of a ruling to secure any of the evidence referred to in paragraph 1, subparagraph 1 from payment of a security deposit.*
5. *Complaints against a court ruling in any of the matters referred to in paragraph 1 shall be considered by the court within 7 days.*
6. *Any securing of evidence shall comply with Article 733, Article 742 and Articles 744 to 746 of the Code of Civil Procedure respectively.*

- **Arts 12-15 E-commerce Act**

Art. 12

1. A service provider who, while providing services by electronic means, including transmission in telecommunications networks of data transmitted by the recipient of the service, or supplies access to a telecommunications network as understood in the Act of 16 July 2004 – The Telecommunications Act – is not liable for the content of the data, if he:

- 1) is not an initiator of the transmission of data,*
- 2) does not select the recipient of the transmission of data, and*
- 3) does not select or modify the information contained in the transmission..*

2. The exemption from liability, referred to in paragraph 1, shall also cover automated and short-term indirect storing of the transmitted data, if this activity aims exclusively to proceeding with transmission, and the data are not stored longer than it is necessary for accomplishment of transmission in the ordinary conditions.

Art. 13.

1. The responsibility for the stored data shall not be borne by the one who transmitting data and providing for automated and short-term indirect storing of the data in order to make them quickly accessible on the request of another entity:

- 1) does not modify the data,*
- 2) uses recognised and usually applied in such activity information techniques determining technical parameters of data access and their updating, and*
- 3) does not interfere with using of information techniques, recognised and usually applied in this kind of activity for gathering information about usage of the collected data.*

2. The responsibility for the stored data shall not be borne by the person, who, respecting the conditions referred to in paragraph 1, immediately erases the data or makes the access to the stored data impossible as soon as he/she receives the message that the data have been erased from the initial source of transmission or the access to them has been made impossible, or a court or any other competent authority has ordered to erase the data or to make the access to them impossible.

Art. 14.

1. The responsibility for the stored data shall not be borne by the person, who, making the resources of a teleinformation system available for the purpose of the data storage by a service recipient, is not aware of unlawful nature of the data or the activity related to them, and in case of having been informed or having received a message on unlawful nature of the data or the activity related to them, makes immediately the access to the data impossible.

2. The service provider, who has received the formal notice on unlawful character of the stored data provided by a service recipient and has made access to them impossible, shall not bear the responsibility to this service recipient for any damage resulting from impossibility to access these data.

3. The service provider, who has received the reliable message on unlawful character of the stored data provided by a service recipient, and has made access to these data impossible, shall not bear responsibility to this service recipient for a damage resulting from impossibility to access these data, if he/she has immediately notified the service recipient of intention to make the access to the data impossible.

4. The provisions of paragraphs 1 - 3 do not apply, if the service provider has taken control over the service recipient in the meaning of provisions concerning the protection of competition and consumers.

Art. 15.

The entity, which provides services specified in art. 12 - 14, shall not be obliged to monitor the data referred to in art. 12 - 14, which are transmitted, stored or made available by that entity.

- **Arts 422 and 439 Civil Code (CC)**

Art. 422 Civil Code (CC)

Not only the person who directly caused the damage shall be liable, but also any person who has induced or helped another person to cause the damage, including those who consciously took benefit from a damage caused to another person.

Art. 439 Civil Code

Whoever is threatened by a direct damage resulting from the behaviour of another person, in particular from the absence of the due supervision over the enterprise or establishment run by that person or the condition of a building or other facilities possessed by that person, is threatened by a direct damage, may demand that person to undertake measures indispensable for averting the imminent danger, and if necessary also to give an appropriate security.

Please note that there is no regulation specifically tailored for online copyright infringements. Art. 79 and 80 Copyright Act are general provisions on copyright infringement and art. 12-15 of the E-commerce Act, introducing safe harbours and the prohibition of monitoring obligations, apply generally to all infringing content (not limited to copyright or even IP rights).

Art. 422 CC is a general tort law instrument, expanding tort liability (for damages) to instigators, those who aid and abet.

Art. 439 CC is a general tort law instrument of preventive liability.

- **Criminal Law provisions: Copyright Act (arts 115 to 118)**

Art. 115 CA

(...)

3. Whoever, in order to gain material benefits in a manner other than specified in paragraph 1 or 2, infringes someone else's copyright or neighbouring rights specified in Articles 16, 17, 18, Article 19, paragraph 1, Article 191, Article 86, Article 94, paragraph 4 or Article 97, or fails to fulfil the duties determined in Article 193, paragraph 2 or Article 20, paragraphs 1 to 4, shall be liable to a fine, restriction of liberty or deprivation of liberty up to the period of up to one year.

Art. 116

1. Whoever, without authorization or against its terms and conditions, disseminates someone else's work, artistic performance, phonogram, videogram or broadcast in the original or derivative version shall be liable to a fine, a penalty of restriction of liberty or deprivation of liberty of up to 2 years.

2. If the perpetrator commits the act specified in paragraph 1 above in order to gain material benefits, he/she shall be liable to a penalty of deprivation of liberty of up to 3 years.

3. If the perpetrator makes the offence specified in paragraph 1 above a regular source of income or organizes or manages a criminal activity, as specified in paragraph 1, he/she shall be liable to a penalty of deprivation of liberty from 6 months up to 5 years.

4. If the perpetrator of the act specified in paragraph 1 above acts unintentionally, he/she shall be liable to a fine, a penalty of restriction of liberty or deprivation of liberty of up to one year.

Art. 117

1. Whoever, without authorization or against its conditions and for the purposes of dissemination, fixes or reproduces someone else's work in the original or derivative version, artistic performance, phonogram, videogram or broadcast shall be liable to a fine, a penalty of restriction of liberty or deprivation of liberty of up to 2 years.

2. If the perpetrator makes the offence specified in paragraph 1 a regular source of income or organizes or manages a criminal activity, as specified in paragraph 1 above, he/she shall be liable to a penalty of deprivation of liberty of up to 3 years.

Art. 118¹

1. Whoever manufactures any equipment or components thereof designated for illegal removal or circumvention of effective technological protection measures preventing from presentation, recording or reproducing works or objects of neighbouring rights, or trades in such equipment or components thereof or advertises them for sale or rental, shall be liable to a fine, a penalty of restriction or deprivation of liberty for up to 3 years.

2. Whoever possesses, keeps or uses any equipment or components thereof as referred to in paragraph 1, shall be liable to a fine, a penalty of restriction or deprivation of liberty for up to one year.

- **Criminal Law provisions: Criminal Code (arts 278 and 299)**

Art. 278 § 2 Criminal Code

§ 1. Anyone who intentionally steals someone else's movable property is liable to imprisonment for between three months and five years.

§ 2. Anyone who, without the permission of an authorised person, acquires someone else's computer software with the purpose of gaining a material benefit is liable to the same penalty.

Art. 299 Criminal Code

§ 1. The provisions of Articles 291 and 292 [penalizing fencing/receiving of stolen property] apply accordingly to computer software.

§ 2. The court may decide on the forfeiture of the items specified in § 1 and in Articles 291 and 292, even if it is not the property of the offender.

2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?

There are no provisions defining the term ‘intermediary’ for the purpose of copyright infringements. Poland has in particular failed to implement art. 8 (3) of the InfoSoc directive. Different types of intermediaries such as access or host providers have been defined in the e-commerce Act, implementing the e-commerce directive. This regulation is however in no way specific for copyright law. Please note that, by their very nature, e-commerce safe harbours cannot impose liability, but provide exemptions from it. Any concept of ‘intermediary’ conceived for safe harbours is therefore not necessarily identical to intermediaries that could be held liable for copyright infringements (though intermediaries recognized by the e-commerce act would most likely be included in such a category).

3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
 - Depends on the commercial or for-profit nature or intent of the use or user;
 - Is uncertain and, if so, why;
 - Varies depending on the type of protected content (music, audio-visual, books, and video games).
- If that is the case, please cite and/or describe as completely as possible the relevant differences.

a) Downloading copyright-protected content from illegal/unauthorized sources on the Internet.

Downloading a copyright work is a copyright relevant use. It can be legalized only by a copyright exception. Generally, the most obvious exception applicable to downloads would be the private use exception (art. 23 CA). Downloading for commercial or professional purposes would be therefore considered infringing. As regards private use, the prevailing view before the *ACI Adam* decision of the CJEU was that the application of this exception did not depend on whether the source was legal. The wording of the relevant provision has not been amended since then, but after *ACI Adam* opinions of legal commentators are not unanimous. Some claim that because the provision stayed the same, downloading from illegal sources remains covered by the exception until the law is revised. Others claim that the interpretation must now ensure conformity with EU law.

In Poland, copyright infringement has never depended on (a) knowledge or awareness (b) commercial nature or (c) type of work. This does not mean such considerations are never relevant: for example, knowledge or awareness may be important for some sanctions, such as damages according to the general principles of civil law (where fault is required); commercial use excludes the private use exception; there is no private use exception for computer programs and electronic databases. ‘This disclaimer may be applied to all the below answers.

b) Streaming copyright-protected content from illegal/unauthorized sources on the Internet.

With streaming the only important difference when compared to downloading would be the lack of a (permanent) copy (although this is debatable). One would have to assume that Polish law must take into account the CJEU’s case law, which would make streaming from illegal sources a form of copyright infringement. It is relatively easy to support this conclusion under Polish law, because in Poland the scope of copyright is very broad. Unlike many legal systems (including EU law), where the scope of copyright is determined by specific exclusive rights (reproduction, distribution, communication to the public), in Poland the exclusivity encompasses any use of a copyright work, creating a presumption that any use is covered by the right (the obvious template is the scope of property rights in civil law). This results from the general clause in art. 17 of the Polish Copyright Act, according to which an exclusive right to use the work and to manage its use throughout all the fields of exploitation and to receive remuneration for the use of the work.’ Specific exclusive rights are only manifestations of this property-like type of protection.

This should not be understood as meaning Polish copyright law does not distinguish between types of exclusive rights. They are recognized and sometimes legally significant (e.g. exhaustion refers to distribution, communication to the public – or, translating literally, dissemination - is also a defined term in the Copyright Act). The law recognizes more detailed “sub-rights” for contractual purposes (art. 50 of the Copyright Act) which are called “fields of exploitation”. The general clause’s consequence is, however, that although the vast majority of copyright relevant uses are covered by the internationally accepted ‘types of rights’, those that are not cannot be automatically considered to lie outside the scope of copyright.

I will use an example of a classic property right from the German Civil Code (the Dutch civil code defines property in a perhaps more modern, but less typical way)

§ 903 BGB:

“The owner of a thing may, to the extent that a statute or third-party rights do not conflict with this, deal with the thing at his discretion and exclude others from every influence. The owner of an animal must, when exercising his powers, take into account the special provisions for the protection of animals.”

There are certainly typical ways of “dealing with a thing”, such as possessing, using, “natural” and ‘civil’ fruits, etc. Some laws (e.g. the Polish civil code in art. 140) list them as examples. But the overarching concept of ‘property’ means such lists are never exhaustive. A copyright related example would be the controversy whether photographing a building infringes somebody’s right of ownership.

A very important question in the light of CJ EU’s jurisprudence is whether such a model is actually possible under EU law. When the court says (in *Svensson*): “Article 3(1) of Directive 2001/29 must be interpreted as precluding a Member State from giving wider protection to copyright holders by laying down that the concept of communication to the public includes a wider range of activities than those referred to in that provision.” this necessarily curtails the freedom of national legislators. It would be difficult to reasonably argue that you cannot define “communication to the public” more broadly than the CJEU does, but you can achieve the same result making an activity that is not a communication to the public a copyright infringement under the general clause.

c) Stream-ripping copyright-protected content.

The same as for downloading.

It would be in my opinion possible to argue, stream ripping circumvents an effective technological measure, although this is not without doubt. The definition of an ‘effective technological measure (art. 6 p. 11 CA: “technological protection measures which enable right holders to control the use of a protected work or an artistic performance through the application of an access code or a protection mechanism, including without limitation encryption, scrambling or any other transformation of a work or an artistic performance or a reproduction control mechanism which serve the protection objective”) is such that the very act of streaming would have to be understood as a ‘protection mechanism’.

d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.

Obvious infringement. (a) of the reproduction right and (b) of the making available right. As to the relation between types of rights and the general clause of art. 17 see above Q1.

e) Posting **hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.**

- *Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard **surface hyperlink**, **deep-link**, **embedded or framing hyperlink**).*

We should probably assume the law has to correspond to the latest European developments. Before CJEU’s case law on linking Polish courts in the rare cases where this mattered were inclined to confirm that linking could constitute communication to the public.

Examples:

- Judgment of the Appeal Court in Krakow, 20 July 2004, I ACa 564/04, TPP 2004/3-4/155. The case concerned the protection of personal interests (reputation) - a deep link constituted a communication of the plaintiff’s image (photo) to the public.
- Judgment of the Appeal Court in Warsaw, 7 May 2014, I ACa 1663/13 – a link that, when clicked, leads to the work being displayed, even in part, constitutes a communication to the public (openly rejecting *Svensson*).

It is not possible to argue that the existing case law clearly differentiates between the types of links. It may be assumed that Polish courts are ready to treat any deep link as a form of communication and do not require additional elements present in embedding, framing, etc.

f) The sale of **Kodi boxes or similar devices.**

Before the *Filmspeler* decision this could not be in my opinion regarded as copyright infringement (though there is no case law to my best knowledge). It could, however, be considered a tort of assisting in copyright infringements (art. 422 CC).

Assuming Polish courts follow the CJEU's approach this could change after *Filmspeler*, but there is no case law yet.

g) Other types of unauthorized online use of copyright-protected content not listed above.

Nothing to report.

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

There is no provision in the Copyright Act to this effect, but one must assume that because copyright infringement is a tort, the general rules concerning liability of minors must be applied. The civil code provides that only persons who are at least 13 years old can be liable in tort. It could be argued – although I cannot cite any authority – that the property-like protection copyright offers (e.g. by way of injunctions) is applicable against everyone, regardless of age. Practically, this is however of limited significance. Obviously, when minors commit infringements, their parents or other legal guardians could be made liable due to the lack of supervision, etc.

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country's law? If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.

Yes, online intermediaries benefit from liability exemptions.

The Polish e-commerce Act implements the safe harbour provisions of the directive 2000/31/EC. For this reason, I will refrain from analysing it extensively, as the essence of the applicable legal rules is comparable to other EU jurisdictions. It is also helpful that arts 12-15 of the directive have been transposed into Polish law by provisions of the e-commerce Act having exactly the same numbers (e.g. art. 12 of the directive by art. 12 of the Polish Act, and so forth). The implementation is, however, not always accurate. The main issues are:

- The fact that art. 15 of the Polish Act, when read literally, would seem to prohibit any kind of monitoring obligations, whereas the directive allows for specific (as opposed to general) monitoring. There are court decisions disregarding this difference in wording.
- The fact that art. 14 of the Polish Act does not distinguish between injunctions and damages and always requires the ISP to have positive knowledge of the infringement (in the directive, as far as claims for damages are concerned, it suffices that an ISP is “aware of facts or circumstances from which the illegal activity or information is apparent”). Again, some court decisions, including the judgment of the Supreme Court of September 30, 2016, seem to disregard this discrepancy.
- According to the directive, a hosting provider should immediately remove or disable access to the illegal information. The Polish Act only refers to “disabling access” (leaving out the “removal” part).

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

The uncertainty has been mainly caused by the CJEU's jurisprudence. This is of course an area where one could submit a lengthy analysis, but suffice it to say that the prevailing view does not (did not) consider the activities of service providers as giving rise to primary liability, unless they knew of the infringing content. In case of knowledge it would be assumed that the service provider concerned (at least a hosting provider) communicates the work to the public and can be liable as direct infringer. To avoid misunderstanding, by knowledge I mean knowledge of a specific work in a specific 'location', not general knowledge that a particular provider's services are used to illegally communicate works (even a large number), or even the same work, but in previously undisclosed accounts.

After *Filmspeler* and *Ziggo* this can change, but it is too early to tell.

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:

- The suspension from the Internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.
- The monitoring or **filtering** of content.
- The **blocking** and removing of infringing content, including notice-and-takedown.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- **Graduated response systems.**

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

All the sanctions referred to below are not specific to the online environment. They are the same regardless of the type of works. I will differentiate between primary and secondary infringements.

a) Civil.

Primary infringers

- Damages, either under general rules of civil law, or as a double license fee. The double licensee fee remedy does not require fault.
- Restitution of profits
- Injunction (stop the infringing actions; refrain from infringement in the future)
- Removal of the effects of the infringement

Secondary infringers

- Damages – according to the courts – only under general rules of civil law, i.e. the actual damage and lost profits, the amount of which must be proven by the plaintiff.
- Preventive injunctions (art. 439 CC)

Apart from that:

- Preliminary injunctions, according to the general rules of civil procedure and art. 80 of the Copyright Act.
- Information claims (art. 80 of the Copyright Act).
- Injunctions against intermediaries as envisaged by art. 8 (3) of the InfoSoc directive are not available under Polish law.

b) Administrative.

There are strictly speaking no administrative measures that could be contemplated as ‘sanctions’ or measures against copyright infringers. There are no graduated response systems, or similar mechanisms.

c) Criminal.

Imprisonment, restriction of liberty, criminal fines (see the criminal provisions cited as answer to the first question). Theoretically, criminal measures aimed at confiscating the means used to commit a criminal offence.

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country’s law against intermediaries to address online copyright infringement by third party users of their services?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

No differences depending of the type of content.

The available measures differ depending on whether an intermediary may be considered an infringer (which generally requires that it knows about specific infringing content, e.g. by way of a notice submitted by the copyright owner).

When an intermediary knows of the illegal act and has not immediately blocked access or removed the infringing content, all civil law sanctions may apply (injunction, damages and damages in the amount of a double license fee, restitution of profits, etc.) – see above.

The measure the purpose of which is to let the intermediary know of the infringing content (such as a notice and take-down request) may be practically close to blocking or removing the infringing content, however, strictly speaking, it is not a remedy. Such a notice means that the addressed

intermediary would start infringing copyright if the illegal content is not blocked and removed and the possible injunctions, etc. would result from this infringement.

In all other cases, the only options would be: preventive injunctions (art. 439 CC) and damages according to the general rules, but in both cases, there are numerous legal and practical impediments that would require a detailed description, but that make such measures very difficult to implement.

Measures such as ‘filtering’ or suspending the infringers’ accounts have not been expressly named in the provisions of law. Monitoring would have to be e.g. presented as “measure indispensable for averting the imminent danger” as understood in art. 439 CC.

b) Administrative.

Nothing to report.

c) Criminal.

If an intermediary is not an infringer, and cannot be proven to have wilfully instigated infringements, or assisted in committing them (knowledge of specific infringement required), no criminal sanctions may be applied.

If an intermediary is an infringer or has intentionally assisted or induced others to commit infringements, criminal sanctions listed above (7 (c)) may apply.

9. To the best of your knowledge, are there significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

No. The differences may be legal – for example a video game contains software and therefore it cannot be argued downloading video games could be covered by the private use exception.

There are also special criminal offences that may be only applied to software (also to works including software, such as video games). – See supra answer to Question 1 (regarding the criminal law provisions).

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

There is no legislation specifically targeting this issue. An intermediary would need a legal ground to disclose such data. There are basically three ways for right holders to obtain it:

- Private enforcement – information claim of art. 80 of the CA. Court practice is not consistent.
- Notifying a law enforcement agency of copyright infringements in order to institute criminal proceedings. If such proceedings are initiated by the public prosecutor’s office, the right holder may participate as the so-called injured party and thus gain access to the files. Public enforcement agencies may require providers to identify users and as parties to criminal proceedings right holders may receive this information.
- Request to the General Inspector of Data Protection (administrative measure)

a) If yes, what conditions must be met for that obligation to arise?

- Private measure – probability of infringement (similar to the standard applied in preliminary injunction cases).

- Criminal – probability that a criminal offence has been committed by a platform or a user.

b) If yes, what type of personal data is typically requested?

IP addresses, other data, when available, that may identify the infringer.

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

Right holders, including exclusive licensees, collecting societies. Professional defence bodies as understood in art. 4 (d) of the Enforcement Directive are not authorized to pursue copyright infringements.

Some criminal proceedings may be instituted ex officio.

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

- Please indicate whether the measures refer to public or private enforcement.

The most widely used measures against infringing users are civil law injunctions and damages in the amount of a double license fee.

Sanctions against intermediaries are rare. They may include: preventing obligations, such as limited monitoring (art. 439 CC) and damages according to the general rules of civil law (art. 422 CC).

In practice, criminal measures usually do not include imprisonment, but only the less severe sanctions.

a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?

No, all these measures have been available for longer than the last three years.

b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.

In the only case concerning copyright infringements by an intermediary the Regional Court in Krakow (judgment of May 27, 2015, IX GC 791/12) awarded damages calculated according to the general rules of civil law, based on art. 422 CC (intermediary as a person wilfully assisting its users in committing a tort) and has imposed monitoring obligations for the future referring to specific copyright works (checking links to infringing content in Google and Bing search engines), based on art. 439 CC (preventive liability).

The defendant's appeal was largely dismissed by the Appeal Court in Kraków (Judgment of September 18, 2017, case file no. I ACa 1494/15). The appeal court upheld the monitoring duties and extended the defendant's obligations by imposing a duty to remove or block access to accounts of repeat infringers.⁴⁹⁹ It should be, however, pointed out that the appeal court considered the defendant

⁴⁹⁹ See also M. Salajczyk, "Poland: File hosting platform ordered to monitor its resources for pirated films", *Lexology* (11 October 2017), available at <https://www.lexology.com/library/detail.aspx?g=b60aab0b-918d-4e81-b005-5e9dcb1e98b6>, describing the injunction in the following terms: "...the court had ordered the service operator to monitor its resources in a very specific way: by 'Googling' itself. Once per month, for the next three years, the employees of the defendant have to search for the phrase 'Chomikuj' + '(title of each film)' + 'film' using Google and Bing search engines. The service

to be a direct rather than indirect (secondary) infringer. The main reason for this was the way the service provider was remunerated for downloads (downloading users had to pay downloading fees for each downloaded file separately). This change of perspective meant that the defendant could not invoke Articles 14 or 15 of the Polish E-Commerce Act. A cassation appeal has been filed by the defendant. The Supreme Court has not yet decided whether it will be heard.

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

The main topics of debate in the last three years have been:

- The obligations of online intermediaries
- The compatibility of the safe harbor provisions of the e-commerce act with EU law
- The missing implementation of art. 8 (3) InfoSoc directive
- The concept of infringement and the difference between direct and indirect infringement
- The impact on CJEU's case law on Polish law, in particular with regard to the linking decisions introducing criteria alien to the fundamental principles of the Polish copyright law, such as the "new public" requirement or subjective elements in the *GS Media* decision, relevant for the very infringement of an exclusive right.

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions/campaigns aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

Yes, there are actions/campaigns aimed at creating awareness of copyright infringements and their consequences. Examples:

- Campaigns organized by the foundation Legalna Kultura (Legal Culture).

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

One of the major issues is that Poland has failed to implement art. 8 (3) InfoSoc (and art. 11, 2nd sentence of the enforcement directive 2004/48/EC), which drastically limits the possibility of obtaining injunctions against intermediaries.

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

There are two reports by PwC and Deloitte on online piracy and its effects in Poland:

- https://www.pwc.pl/pl/publikacje/piractwo/analiza_wplywu_zjawiska_piractwa_tresci_wideo_na_gospodarke_w_polsce_raport_pwc.pdf
- https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Deloitte_Raport_piractwo_june2017.pdf

I am not aware of any credible enforcement statistic regarding online infringements of copyright.

operator is obliged to remove files hosted on Chomikuj.pl that are featured in the first five pages of the search results obtained this way"

Questionnaire Spain

RAQUEL XALABARDER, Professor, Chair of Intellectual Property, Universitat Oberta Catalunya

Last updated: 5 June 2017

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded **red**.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.

The current Act is the Consolidated Text of the Intellectual Property Law, **Texto Refundido de la Ley de Propiedad Intelectual (TRLPI)**, approved by Royal Legislative Decree 1/1996 of April 12, regularizing, clarifying, and harmonizing the applicable statutory provisions.

Boletín Oficial del Estado [BOE] 97 (22 April 1996). A fully updated version of the TRLPI (in Spanish) is available at: <http://www.boe.es/buscar/pdf/1996/BOE-A-1996-8930-consolidado.pdf>
Also available (in Spanish) at the website of the Spanish Ministry of Culture (under the section “Legislación”): <http://www.mecd.gob.es/cultura-mecd/areas-cultura/propiedadintelectual.html>

An English translation of the TRLPI (updated up to 2012) is available at:
<http://www.mjusticia.gob.es/cs/Satellite/1292426984404?blobheader=application%2Fpdf&blobheadervalue1=Content-Disposition&blobheadervalue1=attachment%3B+filename%3DThe+Intellectual+Property+Act+%28Ley+de+Propiedad+Intelectual%29.PDF>

2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?

Spain implemented the Directive on e-commerce by Ley 34/2002, de 11 de julio, *sobre servicios de la sociedad de la información y comercio electrónico* (LSSICE). The LSSICE contains a very broad definition of Internet “**service provider**” as anyone who provides an “economic activity” through the Internet or through any other telematic means; this includes any services provided in exchange for a price, as well as services provided for free, as long as they imply an economic activity. This definition

formally includes ISP which act as “**intermediaries** in the transmission of content through telecommunication networks” (art. 1 LSSICE) and which benefit from the safe-harbor provisions.⁵⁰⁰

In one of the first cases decided regarding safe harbors and copyright infringement, the court accepted that **YouTube was an Internet service provider that qualified as an “intermediary” for purposes of the safe harbors**. In its ruling, the court accepted that the hosting safe harbor was to be applied also to “web 2.0” sites (hosting contents provided by users), not only to web hosting services -as initially envisioned at the time the e-Commerce Directive was passed; and that YouTube was carrying out a “merely intermediary” service, and dismissing any “editorial functions”. See Sent. JM n.7 Madrid, 20 Sept.2010; partially confirmed by AP Madrid (sec.28) January 14, 2014 [*Telecinco v. Youtube*] Westlaw.ES JUR\2014\36900.

3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
- Depends on the commercial or for-profit nature or intent of the use or user;
- Is uncertain and, if so, why;
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

Spain has traditionally adhered to a regime of **strict (objective) liability** for (civil) copyright infringements. Copyright infringements may be unwillingly and inadvertently committed. Knowledge and/or awareness of the illicit activity is not a requisite for the existence of an infringement.

An infringement of copyright (and related rights) may also qualify as a **criminal offence** when it is done with the “intent” to obtain some economic profit (directly or indirectly) and to the prejudice of third parties (art. 270.1 CP). Thus, while intent, knowledge, awareness do not play a role in terms of strict liability for (civil) copyright infringement, they do so under criminal law (copyright crime): it is a requirement for the existence of a copyright crime.

In addition, Act 21/2014 amended the TRLPI to introduce a provision in Art.138 TRLPI allocating liability for copyright infringement (civil and, eventually, criminal) on any Internet service provider that knowingly “induces” the infringement, knowingly “cooperates” with the infringement, or having a direct economic interest in the infringement, has the power to control it.

Art.138 TRLPI: It will also be liable for the infringement, the person who knowingly induces the infringement; the person who cooperates with the infringement, knowing about the infringing conduct or having reasons to know about it; the person who having a direct economic interest in the results of the infringement, has the capacity to control the conduct of the infringer. This does not affect the specific liability exemptions established in Articles 14 to 17 LSSICE, as long as the legal requirements established in them are met.

These are the same instances of **secondary (indirect) liability** (inducement, contributory infringement and vicarious liability) developed by U.S. copyright case law. One may wonder the need for such an alien measure, especially when other existing legal provisions might have sufficed (such as the general doctrine of liability in art.1902 Civil Code: “Anyone who by act or by omission causes

⁵⁰⁰ NB a definition of “intermediary service” is provided for in the LSSICE (Annex b): “an information society service which facilitates the provision or use of other information society services or access to information” and especially refers to the four kind of intermediary services benefiting from safeharbours in the LSSICE.

a damage to another, intervening fault or negligence, is obliged to repair the damage”). The introduction of these secondary liability criteria in the Spanish Copyright Act was prompted by a very much criticised ruling by AP Madrid (sec.28), 31 March 2014 [ManolitoP2P] Westlaw.ES AC\2014\652 which basically absolved the defendant (a website providing P2P software that could be used to access unlawfully posted contents) because he was not committing a direct copyright infringement. See *infra* 3.e).

a) Downloading copyright-protected content from illegal/unauthorized sources on the Internet.

Downloading qualifies as an act of reproduction (art.18 TRLPI); the limitation for private copying (art. 30.2 TRLPI) – “copies [of lawfully disclosed works] done in any support, without third party assistance ... by a physical person exclusively for his/her private use” requires “b) that the copy is made from a lawful source and without contravening any conditions set for accessing the work” and “c) that the copy obtained is not subject to collective or lucrative use or to distribution in exchange for a price.” Accordingly, downloading a copy of a work from an unlawful source or circumventing any DRM or TPM (controlling access or copying, etc.) would not qualify as an exempted private copy.

However, the limitation of private copy expressly excludes the copies done from works that have been “made available to the public online on the basis of an agreement which authorizes the making of a copy and, if applicable, in exchange for a price” (art. 31.3 TRLPI). This means that despite downloading a copy from iTunes may (or may not) be exempted as a private copy depending on the specific terms of the service agreement: the limitation will only apply when the copying is neither authorized nor prohibited by the EULA.

The most recent amendment to the scope of the private copy limitation (art. 31.2 TRLPI) and its compensation (art. 25 TRLPI) has been introduced by RDL 12/2017, of July 3rd, which reintroduced the levy system (after a few years of compensation on the General State budget). Art. 31.2 TRLPI reads as follows:

Artículo 31. Reproducciones provisionales y copia privada.

2. Sin perjuicio de la compensación equitativa prevista en el artículo 25, no necesita autorización del autor la reproducción, en cualquier soporte, sin asistencia de terceros, de obras ya divulgadas, cuando concurren simultáneamente las siguientes circunstancias, constitutivas del límite legal de copia privada:

a) Que se lleve a cabo por una persona física exclusivamente para su uso privado, no profesional ni empresarial, y sin fines directa ni indirectamente comerciales.

b) Que la reproducción se realice a partir de una fuente lícita y que no se vulneren las condiciones de acceso a la obra o prestación.

c) Que la copia obtenida no sea objeto de una utilización colectiva ni lucrativa, ni de distribución mediante precio.

3. Quedan excluidas de lo dispuesto en el anterior apartado:

a) Las reproducciones de obras que se hayan puesto a disposición del público conforme al artículo 20.2.i), de tal forma que cualquier persona pueda acceder a ellas desde el lugar y momento que elija, autorizándose, con arreglo a lo convenido por contrato, y, en su caso, mediante pago de precio, la reproducción de la obra.

b) Las bases de datos electrónicas.

c) Los programas de ordenador, en aplicación de la letra a) del artículo 99.

b) Streaming copyright-protected content from illegal/unauthorized sources on the Internet.

Streaming is not formally mentioned in the TRLPI, but it would certainly qualify as an act of “communication to the public” widely defined in Art. 20 TRLPI as “any act whereby a plurality of people may have access to the work without prior distribution of copies to each of them”;

“communication shall not be considered *public* where it takes place in a strictly domestic environment that is not an integral part of, or is not connected to, a dissemination network of any kind.” Specifically, streaming would qualify as an act of “transmission” either by wire or wireless (Art.20.2(e) and (c) TRLPI).

Art.20(2) TRLPI provides for a non-exhaustive list of acts of communication to the public (mere examples) that cover all the relevant forms of communication brought by technological development over time: (a) stage and public (live) performances, (b) theatrical showing of audiovisual works, (c) wireless transmission, (d) satellite broadcasting, (e) transmission by wire, cable, etc. (f) retransmission (by a different station) by wire or broadcast, (g) emission or transmission of a broadcasted work in a place accessible to the public, (h) public exhibition of works of art or reproductions thereof, (i) making available of works to the public, by wire or wireless means, in a manner that anybody can access them at any place and any time, (j) public access to works incorporated into a database, and (k) any of the aforementioned acts, in relation to a copyrighted database. In short, what defines this right of communication is precisely the fact that it is conducted without any previous distribution of tangible copies of the work. It is not relevant whether the public effectively sees, listens, or anyhow has access to the work; the mere possibility of doing it (without previous access to tangible copies) is enough.

In addition, the streaming copy made in the receiving device will qualify as an act of reproduction which cannot be exempted as a transient/temporary copy under Art. 31.1 TRLPI failing the requirement of “lawful use” as well as lack of “independent economic significance”. Scholars agree on both accounts.

c) Stream-ripping copyright-protected content.

As above, making a copy of the streamed-ripped content would qualify as an infringement of the reproduction right that cannot be exempted as a transient/temporary copy under Art. 31.1 TRLPI. In addition, it would also qualify as an infringement of TPM/DRM (Arts 160-162 TRLPI). Arts 160 and 162 TRLPI implement *verbatim* the protection of technological protection measures and of measures for the management of rights against any acts of removal and circumvention as prescribed in the InfoSoc Directive. The circumvention of a TPM/DRM is considered an infringement of copyright.

d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.

Uploading without due authorization would be an infringement of copyright; specifically, it would qualify as an act of “making available to the public” (Art. 20.2(i) TRLPI).

e) Posting **hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.**

- Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard **surface hyperlink**, **deep-link**, **embedded or framing hyperlink**).

Linking is not formally regarded as an act of communication to the public listed in art. 20.2 TRLPI, but the issue of linking to unlawfully posted contents has been examined by civil and criminal courts. Instead, the provision of links to **lawfully posted contents** has never been addressed by courts.

Initially, the vast majority of Spanish rulings (civil and criminal) held that despite facilitating access to infringing contents, linking did not amount to an act of communication to the public and, accordingly, could not result in liability of the service provider liable; in addition, the safe harbor exemptions also helped in this outcome.

Civil courts concluded that the provision of links does not *per se* amount to either an act of reproduction or an act of making available to the public of the infringing contents. See AP Barcelona (sec.15) July 7, 2011[indice-web.com] Westlaw.ES JUR2011/254296 and AP Barcelona (sec.15) February 24, 2011 [Elrincondejesus.com] Westlaw.ES AC2011/86. Both rulings agree that the provision of links to third party servers allowing *direct or indirect* downloads of infringing contents (via high-speed servers such as Megaupload, on one hand, and via P2P networks, on the other) does not amount to an act of reproduction or of making available.

A landmark case, however, dealt with the distribution of P2P software: Sent. AP Madrid (sec.28), 31 March 2014 [ManolitoP2P] Westlaw.ES AC\2014\652 Phonogram producers sued the owners of websites (www.blubster.com, www.piolet.com, www.manolito.com and www.mp2p.net) that offered three different P2P software (Blubster, Piolet y Manolito) for download, claiming that the software had been developed to “exchange” copyright protected music files and that the websites were expressly inducing users to do so (to infringe copyright); some software could be downloaded for free, but economic profit resulted from download for sale and ads on the websites. Files included infringing phonograms but also files licensed under Creative Commons. The court denied that the defendants were “intermediary service providers” in the sense of the safe-harbors provisions or that could be issued injunctions under art.138 TRLPI because they only developed and market P2P software, they do not conduct any infringing acts and they have not circumvented any TPM/DRM; accordingly, they are not liable for any wrongful use done by users through their software. The court expressly stated that **no “indirect infringement” of copyright** formally exists in Spanish law.

Similarly, most **criminal courts** refused to qualify the provision of links to infringing contents as a criminal offence, concluding that the provider of the links is not engaging in any act of copyright exploitation or simply exonerating the linking website from any copyright liability based on the safe harbors provisions. The landmark case was Sharemula; See Auto AP Madrid (sec.2), 11 Sept. 2008 [sharemula] Westlaw.ES ARP\2008\498; the site offered P2P links to movies and other copyrighted material that could be downloaded by means of a P2P software (eMule) available online, but the court concluded that the website was not communicating to the public (since it was not hosting the infringing files) but only “facilitated” that communication. The court concluded that the website was merely providing “intermediary” services and its liability could be excluded by the safe harbor in Art.17 LSSICE (hyperlinks): as long as it had no “actual knowledge” and there was no “prior ruling” declaring that the linked content was unlawful (notice that the court used a strict construction – notice that this was before the Supreme Court ruling in SGAE, see *infra* answer to Question 5). After Sharemula, almost all criminal cases dealing with links to unlawful contents, were dismissed. See, for instance, Auto AP Madrid (sec.1), 15 March 2011 [edonkeymania] Westlaw.ES JUR\2011\94764. See AP Barcelona (sec.7), 22 Dec. 2005 [todocaraturas] Westlaw.ES JUR 2006\74469.

More recently, especially after the CJEU’s *Svensson* ruling, courts seem to be more comfortable concluding that the provider of links to infringing P2P files cannot be exempted as a mere intermediary (under the safe harbor) and is indeed making unauthorized acts of communication to the public (art.20 TRLPI). There are still plenty of cases absolving defendants for the provision of links to unlawfully posted contents, but here are a few examples that may confirm **a change of tendency**:

- **Criminal Courts**

See AP Valencia (sec.4), 20 Jan. 2014 [Divxonline] Westlaw.ES ARP\2014\179. This is the only ruling where embedded linking has been addressed, even though, indirectly: the court considered that the defendant was doing “something more” (than merely linking) by “providing a program that circumvented the time restriction set for the streaming of movies on the original server” which were shown embedded in their website. The court did not formally rule that embedding the unlawfully streamed contents was an act of communication to the public (in fact, it expressly stated that the provision of links does not constitute an act of communication to the public), but it concluded that the activity of the defendant was a criminal copyright offence. Another ruling

confirming infringement and liability of the website providing links, see Sent. AP Castelló (sec.1) 12 Nov. 2014 [Bajatedetodo.com].

Another ruling by the Supreme Court (criminal chamber) in the case *youkioske* (see below for facts), seems to confirm the change of tendency after the CJEU's *Svensson* ruling on the concept of communication to the public. In this case, the defendant was a website providing links to printed editions of newspapers which had been scanned and posted online; the court expressly mentioned *Svensson* in its ruling.

- **Civil Courts**

See JM n.2 La Coruña, Sent. 247/16, 22 November 2016 [*MediaPro v. RojaDirecta*] Westlaw.ES AC/2017/159 ECLI: ES:JMC:2016:4325; JM n.1 La Coruña, Sent. 24/2014, 1 Feb. 2017 [*DTS/Canal Plus v. RojaDirecta*] ECLI: ES:JMC:2017:5. The defendant Puerto 80 Projects provided several websites offering links to open and free access (via streaming) to sports events broadcasted over pay-TV (restricted-access), and the court has found it constitutes a copyright infringement because it amounts to an unlawful (unauthorized) act of communication to the public (following CJEU's *Svensson* "new public"). In fact, as *obiter dicta*, the ruling adds that the website would also be liable under the indirect liability criteria set in Art.138 TRLPI, as "necessary cooperator" to the infringement to the extent that its service allowed "the big public" to access protected contents stored in websites which were not openly accessible but restricted to subscribers; in summary, the court noted that "without the intervention of RojaDirecta, an average user would not be able to locate the alphanumeric code, despite this code was indexed elsewhere." Furthermore, the court stated that the safe-harbors could not exempt its liability because Puerto 80 Projects was not a hosting provider but a publisher, according to its active role and control over the provision of the links, and its knowledge of its unlawful conduct – thus, implicitly following CJEU's *GS Media* ruling. Previously, precautionary measures sought by the copyright owner against RojaDirecta had already been granted and confirmed based on the same reasons: existence of a "new public" and an unlawful act of communication to the public and no liability exemption under the hosting safe-harbors because of non-neutral activity.

As *precautionary measures*, the websites were closed and the ISP (Internet access providers and DNSS providers) were ordered to block access to the infringing websites; see JM n.1 La Coruña, auto 26 Nov.2015, confirmed by auto AP (sec.4) La Coruña 26 April 2017 ECLI: ES:APC:2017:477A

Liability for copyright infringement deriving from the provision of links to infringing content may also be examined under **the administrative procedure carried on by the Intellectual Property Commission (sec.2) -see infra**. See, for instance, AN (cont.-adm.) 17 Oct. 2014, Westlaw.ES RJCA/2015/15 [elitetorrent.com] where the court expressly referred to the CJEU's ruling in *Svensson* to infer that linking to "unlawfully" posted contents online is an act of communication to the public.

f) The sale of *Kodi* boxes or similar devices.

This has never been assessed by courts and there is therefore not a clear answer. Spanish courts might be tempted to follow the same rationale applied by the CJEU in *Filmstøper*. However, it might also be (more appropriately) examined as a matter of secondary liability, under the criteria introduced in art.138 TRLPI (see *supra*).

g) Other types of unauthorized online use of copyright-protected content not listed above.

Nothing to report.

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

No. Neither the TRLPI nor the CP make any distinction. Parents are responsible for any damages accruing from their kids' acts (while minors) -deriving from either civil or criminal infringements.

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country's law? If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.

Spain implemented the safe-harbors from the Directive on e-commerce by Ley 34/2002, de 11 de julio, *sobre servicios de la sociedad de la información y comercio electrónico* (LSSICE). In addition to implementing -almost *verbatim*- the three **safe-harbors** in the e-commerce Directive (mere conduit Art.14; caching Art.15; hosting Art.16 LSSICE), Spain implemented a fourth safe-harbor for search engines and hyperlinks (Art.17 LSSICE) under the same conditions as those set for the hosting safeharbor.

It is worth mentioning that instead of the standards of "actual knowledge" (for liability claims) and "awareness" (for damages) used in the e-commerce Directive, the LSSICE only uses one standard of "**actual knowledge**" and defines it as "when a competent authority has declared that the data is unlawful... without prejudice of notice and take down procedures in place by virtue of voluntary agreements...". The Supreme Court dismissed a strict interpretation (requiring a prior court ruling) and decided in favor of a flexible (non-strict) reading of the statutory language in the sense that "other means of actual knowledge may be established" so that it is compatible with the EU *acquis*. See *SGAE v. Asociación de Internautas*, STS (civil ch.) 9 December 2009.

ISPs may be subject to civil, criminal, and administrative liability (Art. 13 LSSICE). And despite the LSSICE is silent about the safe harbors not affecting the possibility of issuing injunctions against intermediaries, this is expressly stated in Art. 138 TRLPI as well as in the e-commerce Directive.

The safe-harbor provisions have given rise to abundant **case law** regarding copyright infringement, in civil, criminal, and administrative jurisdictions. For an extensive list of cases (civil and criminal) on ISP liability in Spain, see *Responsabilidad en internet – Blog by MIQUEL PEGUERA*: <https://responsabilidadinternet.wordpress.com/>

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

The scope and conditions for the safe-harbors exemptions are quite straightforward, however, three issues in particular may be more difficult to apply (and generate uncertainty):

- when an ISP activity is "passive and neutral"
- when there is "actual knowledge" for the safe harbor to apply, and
- the indirect liability rules in art.138 TRLPI despite the safe-harbor exemptions.

As a result from the CJEU's rulings in *L'Oreal/eBay* (C-324/09) and *Google France/Louis Vuitton* (C-236/08 to C-238/08) Spanish courts may have to be more restrictive when applying safe harbor provisions (especially, the safe harbor for hyperlinks under Art.17 LSSICE) to web 2.0 ISP, and require that the ISP has a "**passive and neutral**" activity. However, the appeal court in the YouTube case which dismissed Telecinco's appeal, expressly considered the CJEU rulings and concluded that the editorial tasks done by YouTube did not mean that it had active knowledge or proactive control over the files uploaded by its users. As regards the existence of "**actual knowledge**," Telecinco

contended that such knowledge existed on the basis of the several notices sent to YouTube and the Telecinco's logo in the infringing files hosted. The court dismissed that generic notices claiming infringement without identifying the infringing videos was not "actual knowledge" and the Telecinco's logo was also irrelevant. See AP Madrid (sec.28) January 14, 2014 [*Telecinco v. Youtube*] Westlaw.ES JUR\2014\36900.

Another area of uncertainty may result from the new criteria of **indirect liability introduced in Art.138 TRLPI** (in 2014). So far there are no rulings allocating liability to a service provider on the basis of this criteria, beyond the obiter dicta statement made in the ruling of *RojaDirecta*. But it is foreseeable that the courts will need to interpret and apply these criteria which -as mentioned above- have been "imported" from USA caselaw. It also remains to be seen how these criteria will interact with the safe-harbors exemptions: in principle, an intermediary might be exempted from liability (under the safe-harbor) for a copyright infringement committed by its users and, at the same time, found liable for indirect liability (for inducing, contributing or controlling/profiting from the infringement). Besides, notice that safe-harbors are EU *acquis* while the criteria for indirect liability remains a matter for national law only (has never been harmonized).

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:⁵⁰¹

- The suspension from the Internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.
- The monitoring or **filtering** of content.
- The **blocking** and removing of infringing content, including notice-and-takedown⁵⁰².
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.⁵⁰³
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- **Graduated response systems.**

In Spain, IP rights may be enforced in civil courts and criminal courts, depending on the kind of infringement. In all of them, the party who claims the infringement has the burden of proof. In addition, the Comisión de Propiedad Intelectual –CPI (sec.2) is entitled to issue administrative injunctions against ISPs (providers of information society services), which infringe copyright in some specific instances.

⁵⁰¹ The examples listed here are taken from C. Angelopoulos, "European Intermediary Liability in Copyright" (Kluwer Law International 2016), pp. 465 et seq.

⁵⁰² For example, Art. 14 of the E-Commerce Directive includes a notice-and-takedown system in the hosting safe-harbor.

⁵⁰³ For instance, the notices can be posted on the Intermediary's terms and conditions, on the front-page of the platform, as a pop-up message for users of platform, etc. Cf. Angelopoulos 2016, op. cit., pp. 477–478.

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

As a preliminary remark, there are no differences to report. All measures described below are applicable to all types of copyright-protected content.

a) Civil.

<https://www.mecd.gob.es/cultura-mecd/areas-cultura/propiedadintelectual/lucha-contra-la-pirateria/marco-juridico/via-administrativa.html>

The right owner may apply for injunctions to restrain the unlawful activity of an infringer (art.139 TRLPI) and for the adoption of precautionary measures for immediate protection (art.141 TRLPI).

Any of these precautionary measures and injunctions may be sought against the infringer as well as against the intermediaries (regardless of whether they are infringing copyright or not).

Damages may be claimed for any economic and/or moral prejudices caused by the infringement (art.140 TRLPI).

- Injunctions

According to art.139 TRLPI, restraining orders (envisioned for online infringements) may consist of: suspending the infringing exploitation and prohibiting the infringer from resuming it; seizing or sealing any equipment used for the unauthorized communication to the public of works; and suspending Internet services to any person who uses them to infringe intellectual property rights. These measures will include blocking and removing infringing contents.

- Precautionary measures

Precautionary measures may be granted in the course of both civil and criminal proceedings, and simultaneously (art.143 TRLPI), on the basis of two conditions: *fumus bonus iuris* (preliminary assessment in favor of the claimant's rights) and *periculum in mora* (good and reasonable grounds to fear that infringement is imminent and adoption of these measures is necessary to allow effective protection). Pre-trial discovery may also be granted to the author. The granting of precautionary measures will be done according to the general rules of civil and criminal procedure (arts.728 et seq. LEC).

- Damages

Damages may be claimed for any economic and/or moral prejudice caused by an infringement (art.140 TRLPI). According to art.140 TRLPI, damages (monetary relief) will be calculated on the basis of any of the following criteria, as chosen by the claimant:

- the negative economic effects resulting from the infringement (loss of benefits, benefits obtained by the infringer, etc.). The amount of "loss" must be proven, at least, approximately, by objective data;
- the economic amount that the claimant would have obtained, had the exploitation acts been duly authorized (hypothetical license fee). When opting for the "hypothetical license fee" as damages, CMOs tend to multiply their applicable general fees to calculate them; courts have accepted (and modulated) this criterion;

The statutory language is ambiguous as to whether moral damages may be claimed regardless of the regime sought (economic loss or hypothetical license) or only under the first one. The Supreme Court submitted a question for a preliminary ruling regarding this issue (specifically, how to interpret art.13.1 Directive 2004/48/CE) to the CJEU, which ruled in favor of allowing for moral damages to be sought on both accounts (economic loss or hypothetical license). [Case C-99/15 - Liffers, ECLI:EU:C:2016:173]

Moral damages may always be compensated, provided that its existence has been proven and its compensation expressly sought. Moral damages may include “simple moral pain, albeit only within a patrimonial context,” “pain, suffering, worries and trouble,” “anxiety, uneasiness, concern, sadness, melancholy.” An infringement of exploitation rights is not enough per se to infer moral damages. Furthermore, although some case law is tempted to derive moral damages from the mere existence of a moral right infringement, moral damages should not automatically derive from a moral right infringement, either. While the existence of a moral damage must be proven (and expressly sought), there is no need to provide specific evidence of the economic value of that moral damage: the amount of damages will be set according to the circumstances of the infringement, its seriousness, and extent.

The right to bring a claim for damages is available **for a term of five years** from the time at which the claim could have been lawfully filed (art.140 TRLPI); that is, following the author’s or other right owner’s knowledge about the infringement. No term is provided for other claims (injunctions and restraining orders) in the TRLPI, so it is generally accepted that the general term of 5 years provided for in art.1964 Civil Code will apply.

- Measures to identify the alleged infringer, e.g. through injunctions to an ISP requesting the personal information of the infringer may be ordered by civil courts in “special cases.” See *infra* answer to Question 10.

b) **Administrative.**

<https://www.mecd.gob.es/cultura-mecd/areas-cultura/propiedadintelectual/lucha-contra-la-pirateria/marco-juridico/via-administrativa.html>

The Act 2/2011, of March 4, on Sustainable Economy (LES) established an injunction procedure by the Intellectual Property Commission (sec.2) against infringements done for commercial purposes by Internet providers; this procedure was reinforced and enlarged by Act 21/2014 (see *infra* answer to Question 8.b). This procedure is mostly directed towards ISP – see *infra*. Measures include the suspension of the Internet service provided to the infringer, blocking and removing infringing contents, and publication of notices regarding the infringement.

c) **Criminal.**

<https://www.mecd.gob.es/cultura-mecd/areas-cultura/propiedadintelectual/lucha-contra-la-pirateria/marco-juridico/via-penal.html>

According to **art. 270.1 CP**, a **copyright crime** is committed by a person who “with *lucrative intent* and in prejudice of a third party, reproduces, plagiarizes, distributes, communicates to the public or economically exploits in any manner, all or part of a literary, artistic or scientific work or its transformation, performance or execution fixed in any format or communicated by any means, without the authorization of the corresponding copyright owners or their licensees.” In January 2015 (LO 1/2015), Art. 270 CP was amended and “lucrative intent” was substituted with “*direct or indirect economic profit*.”

Accordingly, Art. 270 CP implies the requirement of knowledge (*dolo*) but the cornerstone of this crime is the requirement of “lucrative intent” (in current wording, “direct or indirect economic profit”). It is controversial whether it is satisfied by simply saving money (e.g., when obtaining

infringing copies for free) or whether it requires some sort of active economic (commercial) profit; In general case law (non-copyright) “lucrative intent” has been traditionally interpreted as “any advantage, benefit or use.” However, for copyright cases, this requirement was interpreted restrictively by Spanish criminal courts, as requiring commercial intent, in accordance with the Spanish General Prosecutor’s Circular 1/2006. Circular 1/2006 instructed Spanish prosecutors that, as far as copyright infringements were committed online, criminal sanctions should be reserved for the “most serious cases” where the copyright infringement is committed with a “commercial lucrative intent”. In other words, saving money (getting something for free) does not qualify as “lucrative intent.” This was aimed at avoiding an excessive “criminalization” of society and the overlapping of criminal and civil copyright infringements (and reliefs).

See AP Cantabria (sec.1) February 18, 2008 [Santander] Westlaw.ES ARP2008/262 although this case did not exactly deal with P2P, defendant used several email accounts and chats to offer the “exchange” of musical and audiovisual works for free with other users; the court found no copyright crime in these acts (according to Circular 1/2006), but expressly stated that they do constitute a civil infringement of intellectual property.

In January 2015 (LO 1/2015), Art.270 CP was amended and “lucrative intent” was substituted with “direct or indirect economic profit”; The new wording in Art.270 CP was clearly meant to overcome restrictive readings that kept the majority of users of P2P systems safe from criminal prosecution, however the Spanish General Prosecutor issued a new Circular 8/2015, of 21 December 2015, concluding that -despite the new language- the “economic profit” (be it directly or indirectly obtained) must be of a commercial nature (a “commercial lucrative intent”) and confirming its previous reading that Art.270 CP does not apply to copyright infringers (i.e., P2P users) who are merely saving money.

In general terms, criminal courts have been reluctant to sanction certain copyright infringements under the criminal code for a number of different reasons: the principle of minimal intervention (*ultima ratio*) of the criminal sanction, lack of bad faith by selling counterfeited copies of movies on the street, lack of evidence, or lack of prejudice to the copyright owners. However, this tendency seems to be shifting (perhaps prompted by the 2015 amendment and the CJEU rulings that qualify linking as an act of communication and, in some instances, to the public) and copyright infringements massively conducted online are being condemned by criminal courts.

A recent criminal ruling imposed heavy sanctions on the operators of the website youkioske.com, which offered access to over 17.000 publications of all kind (newspapers, magazines, books, comics, etc) for free; Contents was available on "streaming". The website obtained economic profits by means of advertising banners and video pre-rolls (they obtained 196.280 euros profit). The content was stored on servers in the USA and France: isuu.com (Virginia-EEUU), Youpublisher (California-EEUU) o calameo.com(Paris). Some contents had been scanned (from printed copies bought) and posted online; other was obtained via subscription platforms (such as Orbyt) and then copied and posted; other contents was simply “linked” (hyperlinked) to the original websites. The Supreme Court reversed it, on the grounds that it did not duly take into account the CJEU ruling in Svensson (linking to lawfully posted contents freely available online is not an infringement), and remanded the case to the lower court which confirmed the sanctions of 3 years of imprisonment for each defendant; this time, the ruling was confirmed by the Supreme Court. See AN (criminal chamber) 5 March 2015 Sent.6/2015 [youkioske.com] Westlaw.ES ARP\2015\17; reversed by TS (criminal chamber), 17 Oct. 2015 Westlaw.ESRJ 2015\4803; see AN (criminal chamber) 5.Feb.2016 SAN 117/2016 - ECLI:ES:AN:2016:117; confirmed by TS (criminal chamber) 12 Dec. 2016 - ECLI:ES:TS:2016:5309.

Sanctions for copyright crimes include (cumulatively) fines and imprisonment, depending on whether it is a regular or aggravated crime:

- According to art. 270 CP, the sanctions for **a copyright crime are** (cumulatively) a fine corresponding to 12 to 24 months and imprisonment of 6 months to 4 years. The same penalty applies to any person who intentionally, and without due authorization, imports, exports, or stocks copies of the infringed works, recordings, or performances. This also covers the import of copies (lawfully) acquired in a non-EU member state.

- According to art. 271 CP, the sanctions for the **aggravated copyright crime** (also cumulative) range from a fine corresponding to 18 to 36 months and imprisonment of 2 to 6 years. According to Art. 271 CP, an aggravated copyright crime exists when the profit obtained has major economic effects or the harm caused is particularly serious or the infringer belongs to an organization dedicated (temporarily or permanently) to commit copyright infringements or minors are used to commit these crimes.

In addition, the court may order that the ruling be published in the official journal as well as in any other publication at the expense of the infringer (Art. 272.2 and Art. 288 CP).

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law against intermediaries to address online copyright infringement by third party users of their services?

- *When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).*

As a preliminary remark, there are no differences to report. All measures described below are applicable to all types of copyright-protected content.

a) Civil.

<https://www.mecd.gob.es/cultura-mecd/areas-cultura/propiedadintelectual/lucha-contra-la-pirateria/marco-juridico/via-civil.html>

Injunctions and precautionary measures (see supra) can be sought also against Internet service providers whose services are being used by third parties to infringe, regardless of whether the acts of the intermediaries are infringing or not, and without prejudice to the safe-harbors in the LSSICE (art.138-139 TRLPI).

ISP may be ordered to suspend the Internet service provided to the infringer, block and/or remove infringing contents hosted in its server, and publish notices regarding the infringement.

Since 2014 (Act 21/2014 amending Art.256 Act 1/2000 on Civil Procedure), ISP may also be ordered to provide information to identify the infringer “in some special cases” in civil proceedings. Before that, ISP could only be ordered to provide personal information about their users in criminal proceedings – ex art-12 LSSICE (see infra #10). This is why in a quite exceptional case, an ISP was sued (indirectly) to fight an anonymous infringer: the copyright owner managed to obtain an injunction against an ISP to disconnect the Internet access of one of its clients, an “unidentified” user (acting under the name of “Nito75”) who was infringing copyright through P2P platforms; See AP Barcelona (sec.15), 18 Dec. 2013 [NITO75]. Westlaw.ES JUR\2014\19853

Courts are more reluctant to grant injunctions to prevent future infringements, on account that this would somehow imply an obligation to filter and/or monitor, contrary to the EU *acquis*. For instance, in the YouTube case, the court denied Telecinco's request that YouTube should be prevented to host future infringing contents posted by their users. According to the court, such an injunction would amount to imposing on YouTube **a general obligation to monitor / filter**, which would be contrary to Art.15 e-commerce Directive as well as contrary to the “freedom to conduct businesses” and the “fundamental rights” of users to the protection of their personal data and to access/impart information. See AP Madrid (sec.28) January 14, 2014 [*Telecinco v. Youtube*] Westlaw.ES JUR\2014\36900.

A recent tendency confirms that blocking injunctions may be directly sought against ISPs, rather than suing the individual infringers or websites; this new approach is based on Art.138 TRLPI which

allows that injunctions be also sought against any “intermediaries” whose services are being used to infringe copyright, despite these intermediaries may not be considered infringers themselves.

The AP Barcelona recently confirmed a blocking injunction ordered by the lower court of a website which provided links to infringing phonogram files (www.exvagos.com). The claim was brought by AGEDI (CMO for phonogram producers) against several Internet access providers (Orange, Telefónica, Vodafone, etc). What is “peculiar” about this case is that the claim was brought not as a precautionary measure but as a regular claim, and not against the owner of the infringing website but against several access providers. Despite the direct infringer not being sued, the court accepted that intermediaries could also be enjoined for copyright infringement under Art.138 TRLPI (and expressly referred to the CJEU rulings in *UPC Telekabel C-314/12* and *Scarlet Extended C-70/11* to assess and confirm the proportionality of the measure. See AP Barcelona (Sec.15) Sent. 115/2018 of 20 Feb. 2018 – ES:APB:2018:1317.

b) Administrative.

<https://www.mecd.gob.es/cultura-mecd/areas-cultura/propiedadintelectual/lucha-contra-la-pirateria/marco-juridico/via-administrativa.html>

The Act 2/2011, of March 4, on Sustainable Economy (LES) established an injunction procedure by the Intellectual Property Commission -CPI (sec.2) against infringements done for commercial purposes by Internet providers, which has been reinforced and enlarged by Act 21/2014.

The CPI (sec.2) is entitled to act (issue injunctions) against infringements of two kinds:

- against ISPs that significantly infringe copyright (in order to ascertain whether or not to start a proceeding, the CPI will take into account the audience level of the infringing site in Spain, the amount of works allegedly infringed that can be accessed through it, and its business model);
- and against ISPs that facilitate the finding (location) of infringing contents by means of lists of links (ordered and classified), regardless of whether these links may have been initially provided by the users of the service, when the ISP acts in an “active and non-neutral” manner (that is, beyond a “mere technical intermediary activity”).

If the operator does not withdraw the content or cease its infringing activity, the CPI (sec.2) may order (with prior judicial approval) the infringing ISP to block or remove the infringing contents. It may also order the access provider to stop its service to the infringing site, and order the cancellation of its domain name (when it is a “.es” URL), as well as order the suspension of any payment or advertising services provided (by third parties) on the infringing site. In addition, if the infringer or the ISP do not collaborate and repeatedly fail to comply with the orders issued by the CPI (sec.2), they may be sanctioned with fines of up to €600 thousand.

Any rulings by the CPI (sec.2) must be validated by an administrative court before being ordered; and they may, of course, be appealed. Most of the injunctions adopted by CPI (sec.2^a), validated by a court and appealed, have been confirmed: see AN (cont.-adm.) 17 Nov. 2014 [goear.com] Westlaw.ES RJCA/2015/26; AN (cont.-adm.) 26 Nov. 2014, [multiestrenos.com] Westlaw.ES RJCA/2015/35. See also AN (cont.-adm.) 17 Oct. 2014, Westlaw.ES RJCA/2015/15 [elitetorrent.com]. Only one case was overruled on formal grounds: the injunction was only directed against the provider of the intermediary hosting service and not against the operator of the infringing website. See AN (cont.-adm.) 22 July 2014, Westlaw.ES JUR/2014/205860 [quedelibros.com].

CPI Sec.2^a may not have been as efficient as expected (since 2011, it has only adopted over 40 injunctions). In IIPA’s words: *Unfortunately, Spain’s Intellectual Property Commission (IPC), which has the ability to make the greatest immediate impact in reducing Spain’s online piracy, is also the*

one enforcement tool that the government of Spain has done the least to improve. With an average resolution time of 480 days per case, the IPC is no deterrent to the massive online piracy operations that maintain a firm grip on the Spanish market.

[See SPAIN INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE (IIPA) 2016 SPECIAL 301 REPORT ON COPYRIGHT PROTECTION AND ENFORCEMENT <http://www.iipawebsite.com/rbc/2016/2016SPEC301SPAIN.PDF>].

However, some figures are interesting. See REPORT ON THE ACTIVITIES OF SECTION TWO OF THE INTELLECTUAL PROPERTY COMMISSION (as of June 30, 2017) http://www.mecd.gob.es/cultura-mecd/dms/mecd/cultura-mecd/areas-cultura/propiedadintelectual/lucha-contra-la-pirateria/2017_2Q_Report-Secc2-CPI.pdf

The 124 formally opened files have affected 219 infringing websites:

- 183 websites have been held main responsible of copyright infringement, out of which 56 were linking websites.
- 36 additional linking websites were initially notified as third parties/intermediaries.

The 90 files which were closed due to the disappearance of the object before the formal opening of the procedure have affected 102 additional websites that have taken down infringing contents at the request of the Intellectual Property Commission.

*Thus, the total number of affected websites by the activities of the Intellectual Property Commission adds up to 321. Out of those 321 affected websites, **309 have taken down the infringing contents identified** by the Intellectual Property Commission after the final resolution. Hence, 96.26% of the required websites have taken down the infringing contents. It is important to highlight that the above mentioned figure includes 74 cases where the websites ceased its activities completely:*

- **7 websites with the domain name “.es” have been cancelled** by the public entity Red.es, following the request of the Intellectual Property Commission.
- **40 websites have closed operations** completely following the activities of the Intellectual Property Commission (whether because of information requirements or because of their notification as interested parties after the formal opening of the procedure).
- Moreover, 6 judicial decisions have been taken, giving clearance to **block 27 domain names in Spain** which had been subject of the activities and resolutions of the Intellectual Property Commission.

See also THE ADMINISTRATIVE AND JUDICIAL PROCEDURE CONCERNING INTERNET INFRINGEMENTS: MUCH MORE THAN A SIMPLE NOTICE AND TAKEDOWN PROCEDURE. WIPO/ACE/9/21. DECEMBER 20, 2013 http://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ace_9/wipo_ace_9_21.pdf

c) Criminal.

<https://www.mecd.gob.es/cultura-mecd/areas-cultura/propiedadintelectual/lucha-contra-la-pirateria/marco-juridico/via-penal.html>

LO 1/2015 introduced a new crime against intellectual property (Art.270.2 CP) committed by Internet service providers that, "with the aim of obtaining a direct or indirect economic profit and to the prejudice of third parties, facilitate in an active and non-neutral manner, rather than only doing a merely technical processing, online access to or location of [infringing works or subject matter]..., in particular by providing ordered and classified lists of links to these works and even though these links had been initially provided by the users of their services " (art. 270.2 CP). In short, it is a new crime tailored for websites that offer links to infringing contents (on P2P and other platforms) and regardless of whether their activity qualifies as a copyright infringement or not.

However, as explained in the Preamble, this new crime is not meant to affect those ISPs who provide “merely technical intermediary services, such as neutral search engines” or to those ISPs who only “occasionally link to third party infringing contents”.

9. To the best of your knowledge, are there significant differences in public and private enforcement practices⁵⁰⁴ depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

Beyond the statutory channels provided (civil, criminal and administrative procedures), most CMOs notify service providers about infringing contents available on their websites, advising that judicial claims for copyright infringement will be filed unless the infringing contents is blocked or delisted. Notifications are served upon the individual request of their members who have identified the infringing contents. According to CMOs, ISP tend to comply with these notifications.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

The enforcement of copyright in Spain was severely hindered by the fact that –according to Art.12 LSSICE, ISPs could only be obliged to provide personal information about their users (as alleged infringers) within the context of criminal proceedings, but not in civil proceedings or in order to obtain precautionary measures. This possibility was confirmed by the ECJ ruling of January 29, 2008 [*Promusicae v. Telefónica*, C-275/06]: Member States are allowed to restrict the obligation of ISP to provide personal information to identify infringers to criminal cases (art.15 Directive 2000/31/EC on e-commerce).

To overcome this restriction, Act 21/2014 amended Art.256 Act 1/2000 on Civil Procedure so that - before starting a civil lawsuit for copyright infringement- copyright holders can obtain “in some special cases” personal data of the (purported) infringer or of the owner of a webpage that facilitates the infringement (i.e. by means of links to infringing P2P files). Collaboration (to provide this data) may be sought from the provider of intermediary services as well as from those who provide means of payment or advertising to the (allegedly) infringing pages. This means that personal data of alleged infringers may also be requested from a civil court “in some special cases” – i.e., an “unidentified” user of P2P networks posting thousands of files. For instance, in the NITO75 case reported above, the copyright owner would have now been allowed to obtain personal information of that infringer from the civil court.

a) If yes, what conditions must be met for that obligation to arise?⁵⁰⁵

The obligation to disclose personal data must be ordered by a court, as an injunction or a precautionary measure.

b) If yes, what type of personal data is typically requested?

Name, DNI and personal address to identify the user / infringer.

⁵⁰⁴ In this question, enforcement ‘practices’ refers to the reality of enforcement on the field, including agreements between stakeholders for the enforcement of copyright online (e.g. codes of conduct for notice-and-take-down directed to ISPs that provide a public telecommunications service).

⁵⁰⁵ For example, is such disclosure only possible after a judicial court order, administrative proceedings, or simply at the request of rights holders?

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

The “copyright owner” can claim for copyright infringement and for damages (art.138 TRLPI). In addition, two other instances are envisioned (standing *ex lege*) in the TRLPI:

- CMOs are entitled to enforce copyright (art.150 TRLPI) – once they have been authorized by the ministry of Culture, CMOs can enforce the rights mandated to them in any administrative and judicial proceedings; the CMO does not need to prove individual mandates when suing for copyright infringement of rights that have been entrusted to its management (providing evidence of its authorization suffices).
- An exclusive assignee of rights (art. 48 TRLPI) – when right have been assigned on an exclusive basis, the assignee is entitled to enforce it, regardless of the author’s standing to sue.

The claimant benefits from a presumption of standing to sue (especially, but not only, if he can produce a certificate of registration); the *onus probandi* to defeat such standing or to exclude liability is on the defendant.

Copyright crimes are prosecuted *ex officio* by the General Prosecutor; private parties may join the action as “private accusers” but do not need to. Prosecution occurs upon denouncement or report of infringing activity by an interested party.

Execution of judicial sentences and rulings on copyright infringements is sought and conducted according to the general rules of judicial execution in civil and criminal matters. The party must request execution of the final ruling, and submit a simple copy of it. Execution is usually carried out by the same court that decided on the case (art. 61 LEC).

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

- Please indicate whether the measures refer to public or private enforcement.

a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?

Public enforcement (civil, criminal and administrative) is based on injunctions to block and remove infringing contents, disconnect Internet service of infringers and cancel (or block) .es domain names of infringing sites. Injunctions issued by the CPI (sec.2) may also include (but it does not happen often) the suspension of any payment or advertising services provided (by third parties) on the infringing site as well as sanctions for failing to collaborate.

Criminal sanctions are only now starting to be issued (see YouKioske) and drawing the media attention.

All these measures were introduced by legal amendments taking place in 2011 and 2014 (TRLPI) and in 2015 (Criminal Code).

b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.

- Criminal

Youkioske imposed sanctions of imprisonment to online infringers of **publications** (2016). See AN (Criminal chamber) 5.Feb.2016 SAN 117/2016 - ECLI:ES:AN:2016:117; confirmed by TS (criminal

chamber) 12 Dec. 2016 - ECLI:ES:TS:2016:5309. Measures taken include the seizure of the computer equipment in Madrid, an international injunction to close the website hosted in Canada -although it was not enforced by the Canadian authorities due to “lack of information”- and the blocking of the website through the Spanish Internet service providers (and the changing of access passwords).

Divxonline concluded that the activity of the defendant was a criminal copyright offence because he was doing “something more” than merely linking to **audiovisual contents**, by “providing a program that circumvented the time restriction set for the streaming of movies on the original server” which were shown embedded in their website. See AP Valencia (sec.4), 20 Jan. 2014 [Divxonline] Westlaw.ES ARP\2014\179. Sanctions imposed were imprisonment for 19 months and 15 days, a fine of €7.560 (aprox) and damages incurred.

- Civil

In the *RojaDirecta* cases websites offering links to open and free access (via streaming) to sports events broadcasted over **pay-TV** (restricted-access) were sanctioned for copyright infringement; safe-harbors could not exempt their liability because they were not hosting providers but publishers (they had an active role and control over the provision of the links, and knowledge of unlawful conduct). *RojaDirecta* was sued by MediaPro and by DTS/Movistar+.

- [*MediaPro v. RojaDirecta*] Sent. JM n.2 La Coruña, Sent. 247/16, November 22, 2016 Westlaw.ES AC/2017/159, ECLI: ES:JMC:2016:4325: *RojaDirecta* is *sanctioned* to close all infringing websites and to pay damages to Movistar+; all ISP (any) are ordered to block access to the infringing websites and to deny *RojaDirecta* any service (of hosting, DNS or Internet access); *RojaDirecta* must publish the ruling in two major newspapers (*El País* y *El Mundo*) and on the frontpage of its websites for two weeks.
- [*DTS/Canal Plus v. RojaDirecta*] As *precautionary measures*, the websites were closed and the ISP (Internet access providers and DNSS providers) were ordered to block access to the infringing websites; see JM n.1 La Coruña, auto 26 Nov.2015, confirmed on appeal by auto AP (sec.4) La Coruña 26 April 2017 ECLI: ES:APC:2017:477A / Sent. JM n.1 La Coruña, 1 Feb. 2017 ECLI: ES:JMC:2017:5 *RojaDirecta* is *sanctioned* to close all infringing websites and pay damages to Movistar+.

As mentioned above, a recent tendency confirms that blocking injunctions may be directly sought against the ISP, rather than suing the individual infringer (ex Art.138 TRLPI).

The AP Barcelona recently confirmed a blocking injunction ordered by the lower court of a website which provided links to infringing phonogram files (www.exvagos.com). The claim was brought by AGEDI (CMO for phonogram producers) against several Internet access providers (Orange, Telefónica, Vodafone, etc). What is “peculiar” about this case is that the claim was brought not as a precautionary measure but as a regular claim, and not against the owner of the infringing website but against several access providers. Despite the direct infringer had not been sued, the court accepted that intermediaries could also be enjoined for copyright infringement under Art.138 TRLPI (which and expressly referred to the CJEU rulings in *Telekabel C-314/12* and *Scarlet Extended C-70/11* to assess and confirm the proportionality of the measure. See AP Barcelona (Sec.15) Sent. 115/2018 of 20 Feb. 2018 – ES:APB:2018:1317.

Another interesting ruling (this time, by a lower court) concerns the websites *HDFull* (“<http://hdfull.tv>”) and *Repelis* (“<http://www.repelis.tv>”), which linked to infringing audiovisual contents. The court concluded that the websites incurred in copyright infringement by providing links to illegal audiovisual contents that were carefully edited and classified (the fact that the website contained advertising was also taken into account by the court) and ordered several Internet access providers (Telefónica, Vodafone Ono, Orange, Xfera) to block access to these websites, as sought by

audiovisual producers (Columbia -Sony Pictures, Disney, Paramount, Fox, Universal and Warner). Sent. JM n.6 Barcelona, sent.15/2018, 12 January 2018 - ECLI:ES:JMB:2017:1005.

- Administrative

[PirateBay] upon claim by AGEDI, the CPI (Sec.2) ruling of Sept.2014 was validated by the JCCA n.5 of Madrid on 25 March 2015 and ordered all Spanish Internet service providers to suspend service and block access (within 72 hours) to any website identified as The Pirate Bay group: www.thepiratebay.se, www.thepiratebay.org, www.thepiratebay.net, www.thepiratebay.com. Interestingly, Vodafone received a letter by the CPI (sec.2) informing them of their ruling and proceed to block access to the websites; however, seeing that no judicial ruling was arriving any time soon, Vodafone decided to lift the blocking and allow access to the websites until the judicial order arrived.

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

Online copyright infringement is still high in Spain.

Copyright owners complain about the difficulties regarding the enforcement of copyright online:

- On the one hand, **personal data** about alleged infringers could only be obtained in criminal cases while, on the other, according to the General Prosecutor's Circular, P2P infringements do not qualify as "lucrative intent" for purposes of copyright criminal liability; this put copyright owners in a "cul de sac" position and de facto prevented them from enforcing their copyright against online infringement. To a certain extent, this is the situation that prompted the establishment of the CPI (Sec.2) administrative procedure (in 2011) and its reinforcement (in 2014).
- In the same line, in 2014 an amendment to the civil procedure law allowed personal data to be obtained in "in some special cases" also in civil claims; and in 2015, the Criminal Code was amended to refer to "direct or indirect economic profit" so as to facilitate fighting copyright infringement also in criminal courts; Copyright owners hope that these statutory amendments will help them enforce their copyright and reduce online infringement.
- Other complaints (by copyright owners) refer to the slow judicial processes, including the administrative process (which was supposed to be a "third way" faster and more effective than the traditional judicial way).

From the users' perspective, the debates focus in the (excessive) pricing and the limited lawful offer available.

However, in Spain, the debate on copyright enforcement tends to target the "top manta" (sales of unlawful DVDs and CDs) as well as on the reintroduction of the levy system to compensate for private copying (after a few years of compensation based on the General State budget).

Intellectual Property Rights

*Spanish law protects intellectual property rights, with enforcement carried out at the administrative and judicial levels. Intellectual property protection has improved in recent years and is generally effective although the Spanish government struggles with **significant on-line piracy and rights-holders complain the administrative system is slow due to limited resources.** ...*

Copyrights

Spanish law extends copyright protection to all literary, artistic, or scientific creations, including computer software. Spain has ratified the World Intellectual Property Organization's (WIPO)

*Copyright Treaty (WCT) and the WIPO Phonograms and Performances Treaty (WPPT), the so-called Internet treaties. In 2006, Spain passed legislation implementing the EU Copyright Directive, thereby also making the Internet treaties part of Spanish law. However, **the Internet presents the most problematic area in terms of respect for intellectual property rights in Spain.***

*Spain has undertaken extensive, multi-year reform measures in recent years to strengthen its framework for intellectual property rights (IPR) protections. As a result, Spain now has a strong legal framework and corresponding criminal procedures to address IPR violations. However, **digital piracy in Spain remains relatively high and rights holders continue to voice concerns about the length of Spain's administrative, civil, and criminal procedures for combating online piracy.***

Source: Spain - Protection of Property Rights, (prepared by Export.gov)

<https://www.export.gov/apex/article2?id=Spain-Protection-of-Property-Rights>

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions/campaigns aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

“Cultura en positivo” <http://www.culturaenpositivo.mecd.gob.es/es/index.html> It is an informative campaign prompted by the Spanish Ministry of Culture to foster access to lawful contents online. Basically it states that in order to ensure that culture will subsist, we need to protect all authors and creators; their financial independence is the only way to ensure their freedom to create. “Let not be fooled: there is no other way for culture to be free” It also establishes a “sign” to identify lawful contents and links to lawful websites: http://www.culturaenpositivo.mecd.gob.es/es/oferta_red.html More than 70 businesses are currently using the “sign” cross different sectors: movie, art, e-books, music, videogames.

CEDRO Spanish Center of Reprographic Rights (www.cedro.org), launched a website <http://www.esdelibro.es/> and an educational campaign to encourage reading, textual creation and respect to the author's rights, intended for the whole of the educational community. Among other goals, it aims at educating on the need to respect the rights of intellectual property that allow its development.

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

A relevant issue to bear in mind is the statutory (LSSICE) requirement of “actual knowledge” and, specifically, a prior court or administrative authority order, for the safe harbors (hosting and linking) to operate and the flexible interpretation imposed by the Supreme Court to avoid contravening the EU *acquis*. This restrictive requirement played an important role in the early judicial rulings on safe harbors (see supra) and may still be a reason for uncertainty in the years to come.

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

For more information on Enforcement, see SPAIN INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE (IIPA) 2016 SPECIAL 301 REPORT ON COPYRIGHT PROTECTION AND ENFORCEMENT <http://www.iipawebsite.com/rbc/2016/2016SPEC301SPAIN.PDF>

*Executive Summary: If Spain's success in the fight against piracy were to be measured solely by the **comprehensive legislative reform** that it has undertaken, there is no doubt that the reforms of*

2014 and 2015 would put Spain on the online enforcement map. However, Spain's success as measured by any concrete change in the significant levels of piracy in the country is **still barely perceptible**. A 2015 study shows that, of all of the digital content that Spain's 35 million Internet users consumed in the previous year, 88% of it was infringing. (Tommaso Koch and Fernando Navarro, "88% of cultural content consumed online in Spain illegal, says industry," El Pais (March 10, 2015), http://elpais.com/elpais/2015/03/10/inenglish/1425997747_249854.html). **The demand for creative content is so significant** that, absent such massive levels of piracy, Spain's economy would generate over 29,000 new jobs, and the Spanish Government would realize an additional 627 million euros (\$US687 million) in annual sales and income taxes. The situation is a stark reminder that for rule of law to take hold, particularly in the online space, administrative and judicial enforcement bodies must be equipped with the resources and training to implement the law effectively with the aim of obtaining concrete results.

Questionnaire Sweden

KACPER SZKALEJ, Lecturer and PhD Candidate, Institute of Intellectual Property, Marketing and Competition Law (IMC), Uppsala University

Last updated: 1 June 2018

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded **red**.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.

It is understood that this question primarily concerns the rules relating to the scope of the exclusive rights and limitations.

The primary source regulating online copyright infringement is the *Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk* (Act on Copyright in Literary and Artistic Works⁵⁰⁶, hereinafter “Copyright Act”).⁵⁰⁷

For the sake of completeness, it ought to be noted that the *Internationell upphovsrättsförordning (1994:193)* (International Copyright Regulation) completes the Copyright Act in relation to rules on the applicability of the Copyright Act with regards to other states and interstate organisations in light of Sweden’s obligations under various international instruments, for instance the Berne Convention, Universal Copyright Convention, and the WIPO Copyright Treaties.

2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?

⁵⁰⁶ Non-official English translations of the titles of selected legislative instruments have been provided by the Swedish Government in Ds 2001:7 Ministry Publication Series. This document is used henceforth for the English translation of the title.

⁵⁰⁷ In accordance with OSCOLA, reference to the various legislative provisions will be made in the same format as is used in Sweden, except that an English title will be used. For the sake of clarity, the main components of which a primary source of law is made up of will be referred to as *section* (despite the use of the § symbol in Sweden), whereas the components of a *section* will be referred to as *paragraph*. By way of example, “2§ Copyright Act” denotes section 2 of the Act, whereas 2§ 3 para Copyright Act denotes the third paragraph of section 2 of the Act. Any translations appearing in this questionnaire have been made by the author.

While the term ‘intermediary’ (sv. *mellanhand*) is only used in 11a § Copyright Act which exempts the making of temporary copies from the scope of the reproduction right (and which was introduced to implement Art. 5(1) InfoSoc Directive), the term is not defined in the Act itself, nor does the Act exemplify types of intermediaries. Moreover, the *travaux préparatoires*⁵⁰⁸ to the implementation of the InfoSoc Directive in Sweden also remain silent as to the meaning of this term. Instead reference is made to recital 33 InfoSoc Directive: “a condition for temporary forms of copies to be exempted from the exclusive rights is that the intermediary does not modify the information and does not interfere with the lawful use of technology which is commonly recognised [used] and which is used in the industry to obtain data about how the information is used”.⁵⁰⁹

Nevertheless, in the context of copyright law, Swedish law exempts intermediaries from *financial liability* for the transfer of infringing content where such intermediaries fall within the definition of a *service provider* in 2§ of the *Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster* (E-Commerce Act), implementing the E-Commerce Directive.

For the wording of the specific provisions, please refer to the answer to Question 6 below.

3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
- Depends on the commercial or for-profit nature or intent of the use or user;
- Is uncertain and, if so, why;
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

As a preliminary point it ought to be noted that, notwithstanding the CJEU’s judgements in C-160/15 *GS Media v Sanoma Media Netherlands and Others* and C-527/15 *Stichting Brein v Jack Frederik Willems (Filmspeler)*, Swedish copyright law prescribes strict liability for copyright infringement. As a result, knowledge, awareness, intent, negligence, or lack thereof, or the commercial/non-commercial nature of a copyright-relevant act, has not been relevant for the sole determination of the existence of an infringement. However, all of these factors are relevant for the applicability and scope of different sanctions. Please therefore refer to Questions 7 and 8 below for information on when these factors become relevant.

The above-mentioned decisions of the CJEU have likely affected this default point.

a) Downloading copyright-protected content from illegal/unauthorized sources on the Internet.

The act of downloading constitutes an act of reproduction (2 § Copyright Act provides the exclusive rights) for which consent is normally required. The same applies to content protected by neighbouring rights (46§ and 48§ Copyright Act providing a reproduction right for sound recordings and broadcasts

⁵⁰⁸ Preparatory works have a highly persuasive force in the legal system of Sweden and are used as the main source for the interpretation of primary sources of law.

⁵⁰⁹ Regeringens proposition 2004/05:110, p. 95.

respectively). In the absence of consent, such an act will constitute an unlawful act of reproduction, unless it falls within the scope of the private copying limitation.⁵¹⁰

Notable examples of case law

- NJA 1996 s. 79, Swedish Supreme Court (judgement delivered on 22 February 1996). The Supreme Court noted obiter that the download of an unlawful copy of a work (computer program on the facts) ought to be an infringement of the reproduction right (case concerning copyright liability in relation to the administration of a Bulletin Board System that was used by others to upload and download content).
- Case B 2160-12, Svea Court of Appeals (judgement delivered on 11 April 2013) concerning download (and communication to the public) of films in peer-to-peer networks. Case appealed to the Supreme Court (NJA 2014 s. 859, judgement delivered 9 December 2014) on matters relating to the appropriate level of the criminal sanction.
- Case B16995-11, Göteborg District Court (judgement delivered on 26 November 2013) concerning download (and communication to the public) of sound recordings on a peer-to-peer network (TPB). Case appealed to the Court of Appeals (Case B 5501-13, judgement delivered 16 June 2014) on matters relating to the appropriate level of the criminal sanction.

Applicability of the private copying limitation

Where the work/content in question has been uploaded to the server without the consent of the rightholder (i.e. while the source itself is illegal, so is the actual copy that can be downloaded), the private copying limitation (12 § Copyright Act) will not apply because the copy of the work from which the private copy is to be made must be a lawful copy of the work (12 § 4 para Copyright Act).⁵¹¹ Notwithstanding the ruling of the CJEU in C-435/12 *ACI Adam B.V. and Others v Stichting der Thuiskopie and Others*, it has been an express rule in Swedish copyright law since the implementation of the InfoSoc Directive that 12 § does not apply when the original copy is an unlawful copy.

It ought to be noted that 12 § expressly excludes from its scope reproductions of computer programs⁵¹², (digital) reproductions of compilations in digital form as well as entire books (only limited parts of “literary works in written form” fall under 12 §). Making a private copy of either of these three categories will never be allowed, irrespective of the legality of the source, in the absence of consent.

For the sake of completeness, 12§ contains another requirement for its applicability, which requires that the copy of the work must have been made available to the public in the sense that it has been published (12§ 1 para Copyright Act). Please refer to the answer in point **g**) below.

⁵¹⁰ The Copyright Act uses the term *inskränkning*. This term corresponds to the English term *limitation* rather than *exception*. Moreover, 2§ Copyright Act concerning (all) the economic rights provides in its first paragraph that “Copyright provides, subject to the limitations prescribed hereinafter, the exclusive right to control the work by making copies of it and by making it available to the public...”. As a matter of principle, the exclusive rights ought to be viewed as “islands in an ocean of permitted use”, however the Swedish courts appear to favour a narrow interpretation of the limitations and treating them as *exceptions* instead, while construing the exclusive rights broadly.

⁵¹¹ The provision states that the copy which is to be reproduced cannot have been made in violation of 2§ Copyright Act, i.e. it cannot have been an infringing copy. Such a wording encapsulates the making of a copy on the basis of another limitation, and can therefore be a *lawful* copy. This notwithstanding, it follows expressly from the *travaux préparatoires* to the implementation of the InfoSoc Directive that the copy which is to be reproduced can be a lawful copy. Regeringens prop. 2004/05:110, p. 119.

⁵¹² This will most likely include video games. NJA 2000 s. 580, Swedish Supreme Court (judgement 22 November 2000) categorising a video game as a computer program. Cf. MD 2011:29, Market Court (judgement 29 November 2011) categorising a videogame as a cinematographic work.

b) Streaming copyright-protected content from illegal/unauthorized sources on the Internet.

Prior to the CJEU decision C-527/15 *Stichting Brein v Jack Frederik Wullem (Filmspelers)*, Swedish copyright law did not as such preclude streaming (as defined herein) from illegal/unauthorised sources because the actual act of receiving and/or viewing the streamed content (the result of which would be the creation of a temporary copy) would fall within 11a § concerning the making of temporary copies. Unlike 12 §, this provision does not contain an express requirement of the legality of the copy and was also understood not to contain such a requirement. The *travaux préparatoires* to the implementation of the InfoSoc Directive expressly indicate⁵¹³ that a copy being temporarily reproduced need not be legal copy.

Nonetheless, by virtue of the applicability of CJEU rulings in Sweden, and in particular as a result of the CJEU decision in C-527/15 *Stichting Brein v Jack Frederik Wullem (Filmspelers)*, the act of streaming as defined herein will likely be viewed as an infringement of the reproduction right and will not fall within the temporary copying limitation anymore.

c) Stream-ripping copyright-protected content.

For the purpose of this question it is assumed that the original stream originates from a legal/authorised source. In any other case it will constitute an infringement by virtue of the inapplicability of 11a § and consequentially 12 § Copyright Act.

As the streaming service is lawful, the service provider is dealing with content that has lawfully been made available to the public (i.e. the streamed content does not concern unpublished works). Moreover, and for the same reason, the copy, which is being “caught” by a piece of software for the purpose of subsequent storage as it is streamed, is being transferred with the consent of the rightholder. Neither of the two general requirements pertaining to the status of the copy that 12 § imposes can therefore be seen as precluding an act that results in the creation of a permanent copy of the work from a stream and 12 § will therefore likely apply.

Consequently, Swedish copyright law appears to allow stream-ripping in general in situations where the stream originates from an authorised source, on the basis of 12§, unless the streamed copy is a literary work in written form.⁵¹⁴

To the extent that a user may be required to circumvent technological protection measures (TPMs) as defined in 52b § 2 para Copyright Act (implementing the definition in Art. 6 InfoSoc Directive), the situation is not obvious. It should be noted that 52d § para 2 Copyright Act permits a user to circumvent TPMs if they have “lawful access to the work” and circumvents for the purpose of “being able to watch or listen to the work”. While the argument could be made that in a situation such as the one described the purpose of circumvention is the creation of a permanent copy rather than its consumption, the provision does not require that such consumption be instantaneous nor does the provision require a specific mode of consumption, which as such is not an act falling within the

⁵¹³ Regeringens prop. 2004/05:110, p. 97.

⁵¹⁴ For the purpose of this sentence, it is assumed that a user would be attempting to create a permanent copy of a book that can only be viewed online. For example by taking screenshots of every page and subsequently assembling it to one file. For the sake of completeness, Swedish copyright law imposes a private copying levy on various devices and storage media. Such a levy does not however normally apply to literary works nor to images. Or put differently, it is for the benefit of authors of protected works “which have been disseminated [broadcasted] in radio or TV, or been recorded on a medium” (26k § Copyright Act). Authors of books and images benefit only if the works have been broadcasted over radio or TV (Olsson, H., Rosén, J., *Upphovsrättslagstiftningen – en kommentar*, 4 ed., Wolters Kluwer, 2016, p.236). This is also the reason why books fall outside 12 §. Since a user could likely be assumed to have paid fair compensation in accordance with the requirement of Art. 5(2)(b) InfoSoc Directive when they have legal access to a book over the internet, it appears that Sweden, by excluding books from the scope of 12§, might arguably be in violation of the InfoSoc Directive in this regard.

exclusive rights.⁵¹⁵ In this respect it is worth mentioning that the definition of TPMs in 52b § 2 is *prima facie* narrower than the one in Art. 6(3) InfoSoc Directive for it refers to measures which are *exclusively* aimed to prevent in the normal course of operation “reproduction or making available⁵¹⁶ of the work without the consent of the [rightsholder]”.⁵¹⁷ Since all the requirements for the applicability of the private copying limitation are satisfied, and in any event the consent embedded in the lawfulness of the service warrants at least reproduction in the browser or elsewhere, whenever a user will be potentially reproducing the work in the course of, or following, circumvention, an infringement of the reproduction right does not appear to arise at any point, making it therefore difficult to conclude that a user is performing a copyright-relevant act that they are otherwise not allowed to do.

However, the difficulty of ascertaining the potential applicability of the circumvention exception concerns the meaning of *lawful access* to the work and specifically whether such access must be permanent or whether it can be temporary. In this respect the *travaux préparatoires* to the implementation of the InfoSoc Directive state expressly that such access is intended to refer both to a situation where consent has been received as well as when it originates from any of the limitations,⁵¹⁸ without specifying the duration of such lawful access. Hence, since a subscriber’s lawful access originates both from the rightsholder’s consent and the private copying limitation⁵¹⁹ it appears that such a user has lawful access to the work within the meaning of the circumvention exception.

On the other hand, the *travaux préparatoires* state that “Only if the person has lawful access, e.g. has bought a CD, shall it be permissible to circumvent technological protection, e.g. an anti-copying measure, if it is necessary for the person to be able to listen to the disc”⁵²⁰ which seems to imply that circumvention is only possible when there is an overriding reason such as the impossibility to consume the work without circumvention taking place, despite the existence of lawful access. While this would mean that a user is not entitled to circumvent a technological protection measure when they are able to consume the work without circumvention, it would simultaneously allow a rightsholder to control the modes of consumption, which the legislator has not intended to authorise but leave it instead to the user.⁵²¹

Consequently, it cannot be stated that Swedish copyright law categorically precludes the stream-ripping of a signal to which the user has legal access for the purpose of being able to watch or listen to the work off-line where such stream-ripping necessarily involves the circumvention of a technological protection measure.

For the sake of completeness, users having access to a work “which has been made available to the public in accordance with agreed contractual terms in a way that makes it possible for individual persons to access the work through a communication⁵²² from a place and at a time individually chosen by them”, as opposed to beneficiaries of certain privileged exceptions, are as a matter of law not entitled to apply for an injunction against a rightsholder to make a work available if a TPM makes it

⁵¹⁵ Regeringens prop. 2004/05:110, p. 304 noting that it is not a copyright-relevant act to watch or listen to a copyright-protected work. For the sake of completeness, the term *copyright-relevant act* refers only to the exclusive rights.

⁵¹⁶ In Swedish copyright parlance *making available* constitutes an umbrella term referring to communication of the work to the public, public performance, exhibition and distribution (2 § 3 para 1-4 points Copyright Act respectively).

⁵¹⁷ That measures must *exclusively* prevent acts falling within the economic rights to be categorised as TPMs follows from the introduction of the circumvention exception as such. By introducing the exception, the legislator decided that it was not necessary to simultaneously state that TPMs only prevent infringing acts. Proposition 2004/05:110, p. 304. NB the effectivity requirement referred to in Art. 6(1) and (3) InfoSoc Directive is incorporated into the definition of TPM, i.e. for a measure to be regarded as a TPM it must be effective to begin with. See 52b 2 para § Copyright Act.

⁵¹⁸ Proposition 2004/05:110, p. 304-05.

⁵¹⁹ and arguably the temporary copying limitation.

⁵²⁰ op.cit., p. 304

⁵²¹ ibid. p. 303 stating *inter alia* that if it would not be possible to circumvent an anti-copying measure on a CD which except copying also prevented one from listening to the CD on a computer or a CD-player, rightsholders would receive very far-reaching protection going beyond copyright protection and resulting in an unreasonable and obscure copyright law.

⁵²² Alternatively *transfer*.

impossible to access the work.⁵²³ This strengthens the position of the circumvention exception as the quoted provision indirectly forces such users to rely on their own abilities to circumvent TPMs if they have legal access to the work.

The Copyright Act does not generally regulate contractual relations as far as private consumption is concerned.⁵²⁴ Hence, where the terms and conditions of the service prohibit stream-ripping, a court may be inclined to enforce those terms if it is clear that the user agreed to them. The extent to which the circumvention exception may be excluded by way of contract is unknown to the author. The Copyright Act does not regulate this question. However, if such a possibility were to exist, it would significantly impair the essence of the circumvention exception, rendering it ineffective.

d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.

The sole act of uploading protected content to a website or online platform which is not privately accessible will constitute an act of reproduction and will additionally result in an act of communication to the public once accessible to the public.

NJA 1996 s. 79, Swedish Supreme Court (judgement delivered on 22 February 1996). The Supreme Court noted obiter that the uploading (and downloading) of an unlawful copy of a work (computer program on the facts) ought to be an infringement of the reproduction right (case concerning copyright liability in relation to the administration of a Bulletin Board System that was used by others to upload and download content).

Users have mostly been found liable for communication to the public in cases involving sharing of content over P2P networks:

Case B 2160-12, Svea Court of Appeals (judgement delivered on 11 April 2013) concerning communication to the public (and download) of films in peer-to-peer networks. Case appealed to the Supreme Court (NJA 2014 s. 859, judgement delivered 9 December 2014) on matters relating to the appropriate level of the criminal sanction.

Case B16995-11, Göteborg District Court (judgement delivered on 26 November 2013) concerning communication to the public (and download) of sound recordings on a peer-to-peer network (TPB). Case appealed to the Court of Appeals (Case B 5501-13, judgement delivered 16 June 2014) on matters relating to the appropriate level of the criminal sanction.

Case B838-14, Göta Court of Appeals (judgement delivered on 4 September 2014) concerning communication of sound recordings through DC++. On the facts of the case, the court accepted the argument that the defendant had ripped their CD collection and disliked the rightholders claim of reproduction (there was therefore no initial infringement preceding the communication of works to the public, unlike the previous cases).

e) Posting **hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.**

- *Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard **surface hyperlink**, **deep-link**, **embedded or framing hyperlink**).*

⁵²³ 52f § 3 para Copyright Act.

⁵²⁴ With the exception of 26g § 6 para and 26h § 3 para Copyright Act nullifying contractual provisions that seek to contract out certain permitted uses relating to computer programs (creation of backup copies, observing, studying or testing the function of the program, enabling use of a compilation with its intended purpose; and decompilation of a computer program, respectively).

Prior to the implementation of the InfoSoc Directive in Sweden such linking would have been deemed a *public performance* by virtue of the decision of the Swedish Supreme Court in NJA 2000 s. 292 (deep linking to unlawful mp3 files), and would have been exempted from infringement if the work was a sound recording by virtue of Section 47 of the Copyright Act.

During the implementation of the InfoSoc Directive acts such as those in NJA 2000 s.292 it was decided that linking ought to be categorised as a communication to the public instead of public performance.⁵²⁵ As Section 47 Copyright Act only concerns public performance, such communication were to be deemed an infringement of the communication right.

At the time, a difference was made between surface linking on the one hand (denoted *reference link*) and *deep linking* on the other hand (although the Court used that term, it likely meant *embedded/framed link*), whereby the latter were to be considered an infringement of the communication to the public right.⁵²⁶ It ought to be noted that in the *travaux préparatoires* the term *deep linking* had, regrettably, been defined as “the provision of links to files to other webpages. When someone uses the link it is not apparent that they are moved to another website. For the user it appears as if the content is located on the first webpage”.⁵²⁷ The irrelevance of the type of linking has now however been clarified by the CJEU in C-466/12 *Svensson and Others v Retriever* (see in particular Q3 - and the answer thereto at para [29] - in the application for a preliminary ruling addressing this particular, Swedish, issue).

However, in light of the applicability of CJEU case law in Sweden, Swedish courts will likely follow the same type of reasoning as the CJEU has in C-160/15 *GS Media*. In fact, the District Court of Attunda (Attunda tingsrätt), dealing with a case concerning the posting of an embedded link referring to a YouTube video (homemade) which was unlawfully uploaded to the service, apprehended a very literal and mechanic approach when applying *GS Media*. Particularly the Court stated laconically that

*[Claimant] has denied that the video has been published on YouTube with her consent. Under these circumstances it is [the Respondent] (...) that must evidence the opposite or evidence that the company has in any case not had nor ought to have had knowledge that this was the case. [Respondent] has published the link on a news site and it is, according to this court, obvious that it has occurred with a profit-making aim. [Respondent] is therefore encapsulated by the presumption on full knowledge (...) Respondent has not rebutted this presumption. [Respondent] shall therefore be deemed as having had knowledge that the video was published on YouTube without [Claimant's] consent and has thereby, by making it possible for visitors to see the video via linking to YouTube, communicated the video to the public. [Respondent] has in this way infringed [Claimant's] exclusive right.*⁵²⁸

This author is slightly critical of how the Swedish court has applied the *GS Media* ruling, given the circumstances of the case. Although the final ruling of a court, and especially of lower instance, will in many cases depend on the evidence submitted to it by the parties evidencing their claim, it is noteworthy that the court did not, given the circumstances of the case, consider clause 8 of YouTube's terms and conditions (this point appears not to have been raised), which requires of uploaders to possess the necessary rights. It is common knowledge that YouTube is a very popular site for video sharing and the operators of which make every effort to cooperate with rightholders to combat piracy. How a claimant can possibly rebut the *GS Media* presumption when dealing with a homemade video uploaded to YouTube is incomprehensible.

For the sake of completeness, by virtue of 5§ *Lag (1998:112) om ansvar för elektroniska anslagstavlor* (Act on Responsibility for Electronic Bulletin Boards) the provider (and operator) of a

⁵²⁵ Regeringens prop. 2004/05:110, pp. 70-71.

⁵²⁶ Ibid.

⁵²⁷ Ibid.

⁵²⁸ Case FT 11052-15, Attunda District Court (judgement delivered 13 October 2016), pp. 6-7.

BBS is obliged to remove a message from the service, or otherwise prevent its dissemination, if it is “obvious that the user has infringed copyright or a neighbouring right” by having posted the message.

f) The sale of Kodi boxes or similar devices.

Given the definition of a Kodi box herein (in Annex 1: Legal Questionnaire, *Glossary of Terms*), the sale of such boxes will likely not constitute an infringement in Sweden. While there is no Swedish case law relating to the sale of such devices, the sale of such devices, as such, is not a copyright-relevant act falling within the exclusive rights in 2§ Copyright Act.⁵²⁹ At the time of writing there are many different devices of this type, including devices other than devices running the KODI system, on sale in Sweden, for instance AppleTV, and Google Chromecast.

However, by virtue of the applicability of CJEU case law in Sweden, a Swedish court will likely apply the same reasoning as the CJEU did in *C-527/15 Stichting Brein v Jack Frederik Wullems* when faced with identical circumstances. It therefore appears that where the seller is marketing a Kodi box as allowing the reception of illegal streams and where that possibility is indeed provided by default, such acts ought to be viewed as a communication of the work to the public. In any other case it is unlikely that it will fall within primary infringement.

Such an act could however fall within secondary liability and will attract criminal sanctions where the seller has at least been grossly negligent (see further the answers to Questions 7 and 8). To this end courts have found for example ISPs to be secondarily liable for copyright infringement: Case Ö7131-09 and Ö8773-09, Svea Court of Appeals (judgement delivered on 4 and 5 May 2010); Case PMT 11706-15, Patent and Market Court of Appeals (judgement delivered on 13 February 2017).

g) Other types of unauthorized online use of copyright-protected content not listed above.

Download of unpublished works from lawful source⁵³⁰

§12(1) Copyright Act

The private copying limitation will not apply where the copy is a lawful copy but which has not been previously published. Works are considered published when they have been made available to the public (8 § Copyright Act).

Possible communication to the public by linking when work uploaded with consent of rightholder who has intended to restrict access to the work by using a payment wall but where that wall is not circumvented in fact.

Where a link is provided to a work that has been uploaded to a website with the rightholder’s consent but where access to the work has been restricted, and where that link provides nevertheless access to the work, that link will be deemed to communicate the work to the public. Following the CJEU decision in *Svensson*, infringement of the communication right will be deemed to have occurred in such a case. This was expressly confirmed by the Swedish Supreme Court by judgement of 29 December 2015 in case B3510-11 (see also the CJEU case C-279/13 *C More Entertainment v Sandberg*; the linking questions were however, regrettably, retracted by the Swedish Supreme Court following the *Svensson* ruling) in which the Court held that “...a link that makes it possible to circumvent such a restriction [payment wall] constitutes communication to the public” but continued “This is also the case where the restriction is not a technological hindrance” (paragraph 15 of the judgement).

⁵²⁹ Unless the sale could fall within the distribution right. This would however require that the protected content be stored on, or be part of, the Kodi Box.

⁵³⁰ The term “lawful source” refers in this context to a bona fide service, e.g. where the service as erred in clearing the rights but makes a work available to its users which purchase the work and download, such works not having been published (put into circulation) earlier. Although the service will be liable, so will the users who download as they cannot rely on the private copying limitation even though the copy is coming from a bona fide service.

The facts of the case were that in order to gain access to the content, visitors had to register themselves on the webpage, accept the terms of use and pay for access. Once payment was made, the user would receive “access to a clickable link with the address to the [legal] streaming server” (paragraph 1 of the judgement). It transpired subsequently that the same address was used for the streamed content (live hockey matches), but was later rectified, and that link was made available on the respondent’s website and was deemed by the Court to constitute communication (of subject matter protected by related rights) to the public.

Although the Supreme Court indicated that a restriction does not have to be technological in nature (the CJEU’s judgement in *Svensson* does not appear to preclude this), it is not clear what is applicable if such a link does not in any way circumvent an access restriction. Surprisingly this is exactly what happened on the facts because the payment wall protected *access to the webpage on which a link to the streaming servers was placed* (and not the webpage on which the streamed hockey matches were located), however the Court did not discuss what should be understood by the word *circumvent* or ‘a non-technological hindrance’, and seems to have assumed that as long as there is some form of access restriction which the rightholder has intended to put in place, however (in)effective, making the work available through a link will constitute a communication to the public.

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

Not in particular. The Copyright Act does not contain any particular rules regulating the liability of minors for copyright infringement. As a matter of principle, it is therefore possible for a minor to be liable for copyright infringement. Moreover, the *Skadeståndslag (1972:207)* (Torts Liability Act – a more accurate translation of the title is *Damages Act*), which compliments the Copyright Act in relation to certain remedies, provides in 2 Ch. 4§ that any person under the age of 18 that causes harm to another (including economic harm) shall compensate the harm “to the extent it is reasonable, having regard to their age, development, nature of the act, existence of liability insurance and other economic relationships and other factors”.

For the sake of completeness, 3 Ch. 5§ Torts Liability Act prescribes that parents who have custody over their children shall compensate personal or property harm (*sakskada*). This provision does likely not encapsulate copyright infringement (e.g. reproduction or communication of works to the public) as the word *sak* (eng. *thing*) usually refers to tangible items (chattels).

In case of criminal liability for copyright infringement, the Penal Code prescribes certain age limits. Criminal liability is however not excluded (unless a person is under 15 years of age; 1 Ch. 6 § Penal Code), and criminal proceedings for copyright infringement have been initiated where a person is 15 years old. Please refer to the answer in Question 7 below for the specific age limits and their relation to criminal sanctions and examples of case law.

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country’s law? If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.

Yes. Intermediaries may benefit from the general temporary copying limitation in 11a§ Copyright Act, implementing Art. 5(1) InfoSoc Directive, and by the safe harbour provisions found in the E-Commerce Act, implementing Arts 12-14 E-Commerce Directive. Additionally, where criminal

liability may arise as a result of contributory acts, a party might be absolved from such liability under an unwritten principle (exception) of social benefit (*social adekvans*).⁵³¹

11a§ Copyright Act mirrors to some extent Art. 5(1) InfoSoc Directive and provides the following:

11a§

Temporary forms of copies of works may be reproduced, if the reproduction is an integrated and essential part in a technological process and if the copies are transient or are of incidental importance in the process. The copies must not have an independent economic significance.

Reproduction of copies is permitted under the first paragraph only if the sole purpose of the reproduction is to make possible

- 1. transfers in a network between third parties through an intermediary, or*
- 2. lawful use, i.e. use which occurs with consent from the author or their rightholder, or other use which is not unauthorised by this Act.*⁵³²

The first and second paragraphs do not give a right to reproduce copies of literary works in the form of computer programs or compilations.

As can be noted, 11a § does not apply to computer programs nor compilations. Given the judgement of the CJEU in C-355/12 *Nintendo and Others v PC Box and 9Net*, whereby a video game, for the purpose of application might fall under the system established by the InfoSoc Directive instead of the Software Directive, there might be some uncertainty as to whether video/computer games are encapsulated by 11a § or not.

The safe harbour provisions excepting the liability of intermediaries in specified cases are provided in 16-19§§ E-Commerce Act. For the provisions to apply, an intermediary must fall within the definition of a *service provider*.

Service providers are defined in 2§ of the Act as “physical or legal persons that provide an information society service”, such service being “normally provided for remuneration and which are provided from a distance, electronically and on the service subscriber’s request”.

The safe harbour provisions, implementing Arts 12-14 E-Commerce Directive, are formulated in the following way:

*(mere conduit)*⁵³³

16§ A service provider that transfers information which has been provided by a service subscriber in a communication network, or that provides access to such a network, shall not because of the contents of the information be liable to compensate the harm or pay a penalty, on condition that the provider does not

*initiate the transfer,
selects the recipient of the information, or
selects or changes the information.*

Transfer and provision in the first paragraph also includes such automatic, intermediate and temporary storage of information that occurs only to carry out the transfer, on condition that the information is not stored longer than what is reasonably required for the transfer.

(caching)

17§ A service provider that transfers information which has been provided by a service subscriber in a communication network shall, for such automatic, intermediary and temporary storage that occurs only to make the transfer to other service subscribers more efficient, not because of the

⁵³¹ *Social adekvans* is a legal technical term but is often translated, somewhat erroneously, into *social adequacy*. For the sake of convenience it will be referred to as a *principle*, even though there is disagreement as to whether it ought to be categorised as a principle, exception or a “fail-safe”.

⁵³² C-355/12 *Nintendo and Others v PC Box and 9Net* at [23].

⁵³³ Headings provided by author.

contents of the information be liable to compensate the harm or pay a penalty, on condition that the service provider
does not change the information
satisfies applicable terms for access to the information
follows the rules concerning the updating of the information adopted within the industry branch
does not interfere with the technology, adopted by the industry branch, used to receive data about the use of the information, and
prevents without delay the further dissemination of the information, as soon as the provider receives knowledge that the information that was originally transferred was removed or made inaccessible, or that a court or public authority has decided that this shall occur.

(hosting/storage)

18§ A service provider that stores information which has been provided by a service subscriber shall not because of the contents of the information be liable to compensate harm or pay a fine, on condition that the provider
does not know of the illegality of the information or activity and, when it comes to liability to compensate harm, is not aware of facts or circumstances which make the illegality of the information or activity obvious, or
prevents without delay the further dissemination of the information as soon as he receives knowledge or awareness.

The first paragraph does not apply if the service subscriber that provided the information acts under the service provider's direction or authority.

19§ A service provider that transfers or stores information for another may be found liable of a crime relating to the contents of the information only if the crime has been conducted intentionally.

As can be noted, the safe harbour provisions only absolve an intermediary from compensatory damages or administrative penalties. Neither Act defines nor exemplifies specific intermediaries.

In Case B 4041-09 (judgement delivered on 26 November 2010) concerning the (criminal) secondary liability for copyright infringement of the operators of ThePirateBay, the Svea Court of Appeals while considering TPB to fall within the definition of a service provider in the E-Commerce Act, found that 19 § was applicable on the facts and did not exempt the operators of the service from (financial) liability.

Social benefit (*social adekvans*)

A defendant may be absolved from liability under certain special circumstances if the act can be said to do more good than cause harm. Essentially, where an act involves conscious risk taking and produces a harmful effect, it may nevertheless be allowed on consideration of factors such as the type of risks, the values targeted by the risks, the social value of the act, and the precautionary measures which have been possible and justified.

In relation to ISPs specifically, the *travaux préparatoires* to the implementation of the E-Commerce Directive provide that:

To carry out the activity as such must – inter alia against the background of a well-functioning infrastructure relating to information technology – be considered as socially beneficial [i.e. falling within the principle]. The risks that are attached to the provision of the service (inter alia that one is contributing to the dissemination of illegal information) are such that the risk taking must be deemed permitted.⁵³⁴

⁵³⁴ Regeringens prop. 2001/02:150, pp. 89.

In the criminal liability (contributory infringement) case against the operators of TPB, the court had developed four criteria to determine whether TPB service could benefit from the no-liability principle (Case B 4041-09, p. 24):

1. *Is the character of the service primarily a useful tool for legal use?*
2. *Is the character of the service primarily beneficial for society?*
3. *Does the legitimate use dominate?*
4. *Have precautionary measures been taken, despite the unavailability of infringement?*

In applying these criteria (generally), the Court first recognised that the service had for the most part been used to share music, films, games and other content, and noting that it was difficult to establish the extent to which such content was made available with the consent of the rightholders, felt itself forced to presume that the number was not insignificant. The Court therefore asked whether the legitimate interests of those rightholders to use TPB as a distribution channel for their works, and the equally relevant legitimate interests of users to easily and freely consume culture and entertainment weighs “so much” that, given an overall assessment of the relevant values and existing risks at stake, it is reasonable to not deem the provision of such a service punishable.

While the witness testimony indicated that it was as much legal content as there was illegal content, the Court considered that the various warning letters, screen shots, evidence relating to the number of downloads, and e-mail correspondence between the defendants, evidenced that, irrespective of the proportion of legal and illegal content, the sharing of protected content without the consent of the rightholders was the dominating activity among the users of TPB; and noted that no precautionary measures had been taken, not even after detailed indications and warning letters. The Court therefore concluded that the clearly obvious risk that the activities would lead to a massive infringement of the rightholders’ fundamental rights weighed against the socially beneficial interest to provide a service for file sharing of legal content did not permit it to absolve the operators from liability.

This principle might however have lost its relevance in cases involving intermediaries, because the Patent and Market Court of Appeals (PMÖD) in PMT 11706-15, delivered on 13 February 2017, concerning the first website blocking injunction against an ISP, did *not* address the applicability of this principle at all, despite the fact that the first instance court, the Patent and Market Court (PMD), had not only considered the principle, but held that it was applicable (!) and as a result did not issue the injunction (which would have required a finding of contributory liability).⁵³⁵

While PMÖD went in a completely different direction that PMD (focusing almost the entire judgement on the applicability of Art. 8(3) InfoSoc Directive and *UPC Telekabel*, which PMD did not do), a possible explanation for not considering the social benefit principle might be that this was solely a civil law case *and* PMÖD had departed from established practice to determine contributory infringement on the basis of the requirements in criminal law (introducing instead a civil law definition of contributory infringement). See the answers to Question 8(a) and 12(b) for further details on the case.

For the sake of completeness, in joined cases Ö7131-09 and Ö 8773-09 (decision delivered on 4 and 5 May 2010), concerning the issuing of a preliminary injunction against TPB’s ISP to block Internet access, the Svea Court of Appeals did not discuss the applicability of the principle, despite having applied the criminal law definition of contributory infringement. See the answer to Q6 below for further details of the case.

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

⁵³⁵ Case T15142-14, Patent and Market Court (judgement delivered on 27 November 2015), pp. 26-27.

Whether an act will either fall within the safe harbour provisions or will instead be deemed an act of primary liability has not generally proven to be difficult.

While the interface of copyright liability and the safe harbour provisions is not clearly spelled out in the E-Commerce Act, any relevant difference between an act being categorised as primary liability or instead benefiting from a safe-harbour provision appears to simply concern the remedies that are available to rightholders (for a detailed answer as to the remedies available, please refer to the next part of this questionnaire). The fact that an intermediary's activity may fall within the ambit of either of the safe harbour provisions does not as such preclude injunctive relief against an intermediary, nor any other non-monetary sanctions. Such injunctions, including preliminary injunctions, can, however, only be granted in Sweden if an intermediary is primarily or secondarily liable for copyright infringement (53b§ Copyright Act). *For clarification on the scope of 8(3) InfoSoc Directive vis-à-vis Swedish Law see infra the preliminary remarks to Question 8.*

In this respect, Swedish courts have been consistent in apprehending a broad approach to finding that intermediaries such as ISPs which merely provide Internet access are secondarily liable for copyright infringement.

In particular in joined cases Ö7131-09 and Ö 8773-09 (decision delivered on 4 and 5 May 2010) the Svea Court of Appeals, affirming the decision of the Stockholm District Court, held that a preliminary injunction can be issued against an ISP providing Internet access for ThePirateBay (the operators of which had, at the time, prior to the decision, been convicted of secondary infringement). The Court, having relied on 23 Ch. 4§ Penal Code, noted that an intermediary can be secondarily liable for copyright infringement if it knows about the illegality of the content and has the possibility to, without unreasonable sacrifice, prevent the dissemination of the content, but refrains from doing it. On the facts of the case, the Court held that while it was clear that the ISP provided Internet access to ThePirateBay, they had received knowledge about the illegality of the content as a result of the earlier criminal case against the operators of TPB, and granted the preliminary injunction against the ISP. In this particular case, interestingly, while 16§ E-Commerce Act does not require any knowledge of the illegality of the content for mere conduit, neither the District Court nor the Court of Appeals made any reference to the E-Commerce Act generally or that provision specifically.

Similarly in 2017, the Patents and Market Court of Appeal in allowing an injunction against an ISP to block TPB website, found the ISP secondarily liable for copyright infringement (Case PMT 11706-15, delivered on 13 February 2017, further mentioned below).

While the issue may be insignificant in the sense that the E-Commerce Act absolves from financial liability, and the rightholders did not apply for compensation in these cases, the legal circumstances nevertheless force an intermediary to contest secondary liability claims.

However, as a result of the recent CJEU decisions in *GS Media*, *Filmspieler*, and *Ziggo*, the combined effect of which appears to be a clear broadening of Art. 3 InfoSoc Directive, the interface of primary and secondary copyright infringement, the latter of which has traditionally fallen solely within the competence of Member States, has been exacerbated. Since intermediaries have traditionally been seen in Sweden as secondarily liable for copyright infringement, many types of conduct that would have been deemed secondary infringement might now be deemed primary infringement. This has important consequences for the determination of the strength and breadth of available remedies.

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison

sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:

- The suspension from the Internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.
- The monitoring or **filtering** of content.
- The **blocking** and removing of infringing content, including notice-and-takedown.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- **Graduated response systems.**

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

It is understood that this question concerns foremost an act that, given the identity of the infringer, and therefore its character, appears to fall within primary infringement.

- Damages – sv. skadestånd

Damages for primary copyright infringement are primarily of compensatory nature.

54§ Copyright Act contains the special rules for damages for copyright infringement. These are however complimented by the general principles in the Tort Liability Act.

An important limitation of the scope of 54§ Copyright Act is that it does not apply to reproductions of protected content that violate 12§ 4 para Copyright Act, i.e. reproductions made for private purposes where the copy that is being reproduced is not a lawful copy, unless such reproduction has been made intentionally or with gross negligence. This follows expressly from 54§ 4 para Copyright Act.

54§ 1 para Copyright Act imposes a compensatory rule arising from strict liability connected to the bona fide, but unlawful, use of the protected content. In particular, anyone who unlawfully uses a work must pay an "equitable remuneration" for such use to the author or the rightholder.

However, by virtue of 54§ 2 para Copyright Act, where the de facto infringer has acted intentionally or has been negligent (not grossly negligent), they will be liable to compensate any further damage that the infringement has resulted in. Liability to pay compensatory damages will therefore only arise when the infringement has been carried out intentionally or with negligence.

When setting the amount of payable compensation, 54§ 2 para requires that the court considers

1. lost profit
2. unjust enrichment (profit that the infringer has made)

3. harm to the reputation of the protected content
4. non-economic harm
5. the author's or rightholder's interest that infringements do not occur

For the sake of completeness, exemplary (punitive) damages are not available in Sweden.

- General injunctions (for infringements) – sv. vitesförbud

The Copyright Act does not distinguish between different forms of injunctions (e.g. prohibitive and mandatory, blocking orders etc.). Instead, the relevant two provisions are general to accommodate the flexibility that may be necessary given the circumstances of a case. As a result, the actual formulation of an injunction described hereunder will in every case depend on the evidence submitted (with consideration of the general principles embedded in Art. 8 InfoSoc Directive).

By virtue of 53b§ para 1 Copyright Act a court may issue an (final) injunction against anyone who infringes copyright, or contributes thereto.

By virtue of 53b§ para 2 Copyright Act a court may also issue an interim injunction against an infringer (or contributor thereto) pending the final outcome of the case. 53b§ para 2 further requires the provision of security (collateral) in order to discourage frivolous lawsuits. However the court may exempt a rightholder from providing security if they have limited financial resources.

For a preliminary injunction to be granted, the applicant must show “probable cause” for infringement and that it can be “reasonably feared” that the respondent, by continuing with the infringement, will reduce the value of the exclusive right. Applications for interim injunctions after three years from the date of (ongoing) infringement will likely not satisfy the latter requirement (Market Court 1996:37, judgement delivered on 1 January 1996, reversing the decision of the first instance court and refusing to grant a preliminary injunction after 3 years).

An interim injunction will remain in force even if the case is appealed. The higher instance court may however discharge the injunction.

- Special injunction ordering the provision of information (information injunction) – sv. informationsföreläggande

The implementation of Art. 8 Enforcement Directive did not update existing sanctions and remedies, but led instead to the introduction of a new and independent form of sanction in Swedish copyright law, regulated by 53c – h §§ Copyright Act, the purpose of which is to order the provision of information about infringement. As the injunction is a sanction in it itself, its purpose is not only to allow a claimant to receive further information during an ongoing case (which appears to be its main purpose under Art. 8 Enforcement Directive). Relevant claimants may instead directly apply for such an injunction (53e § 1 para), even though no infringement case is pending.

In particular, 53c § Copyright Act provides the following:

If a claimant shows probable cause that someone has (...) [infringed the economic and moral rights, violated the testament of the author or imported to Sweden for the purpose of distribution to the public copies which have been reproduced abroad under such circumstances that the reproduction would have been punishable in Sweden, or attempted or conspired to commit a crime], the court may, under penalty of a fine, order anyone listed in the second paragraph to provide to the claimant information about the origin and distribution network of the items or services that the infringement or violation concerns (...). Such an order may be sought by the author, their rightholder or [a licensee] (...). The order may only be granted if the information can be assumed to facilitate the inspection of an infringement or violation which concerns the items or services.

The obligation to provide information applies to anyone that has

1. *carried out or contributed to the infringement or carried out or contributed to the violation,*
2. *exercised control over the relevant item on a commercial scale,*
3. *exercised control over the relevant service on a commercial scale*
4. *provided an electronic communication service or other service on a commercial scale which has been used to carry out the infringement or the violation, or*
5. *been identified by someone in 2-4 as having participated in the manufacturing or distribution of a relevant item, or the provision of a relevant service.*

Information about the origin and distribution network of the items or services may particularly include

1. *names and addresses of manufacturers, distributors, suppliers and others that have been in possession of the items or provided the services*
2. *names and addresses of intended wholesalers and retailers, and*
3. *information about how much has been manufactured, delivered, received or ordered, and what price has been decided for the items or services.*

(...)

An important feature of this provision, as can be observed, is that it also applies to direct infringers, rather than merely to secondary infringers or intermediaries. Additionally, the infringement or violation need not be intentional nor negligent, and it may even be issued for attempted or conspired infringement.

By virtue of 53d § 2 para Copyright Act, the obligation in 53c § to provide information does not however apply to information the disclosure of which would reveal that the information provider or their relative has committed a crime.

As a general limit to the possibility to issue such an injunction, 53d § 1 para prescribes that it can only be issued if the reasons for the measure outweigh the “inconvenience or other harm that the measure would cause the party affected by it or any other opposing interest”.

- Special injunction requiring the dissemination of information about judgement

A special measure, implementing Art. 15 Enforcement Directive, is available under 53h § 1 para Copyright Act, whereby a court may order, on application by the claimant, a primary or secondary infringer to pay for appropriate means to disseminate information about the judgement in question. This measure is also available in case of attempted or conspired infringement.

- Change or destruction of property or means used to infringe

Given the specific context of this question, by virtue of 55 § 1 para Copyright Act a court may, having regard to the requirement of reasonableness, order the recalling from the market, change, destruction of, or any other measure with regards to, infringing property or means used, or being intended to be used, to infringe any of the rights.

This will also be available in case of attempted or conspired infringement (55§ 2 para).

- Infringement investigation (preservation of evidence) – sv. intrångsundersökning

56a – 56h §§ Copyright Act, implementing inter alia Art. 7 Enforcement Directive, permit the court to order the carrying out of an investigation against a primary or secondary infringer (or in case of alleged attempt or conspiracy) in search of “objects or documents which can be assumed to be of relevance” for an enquiry about the infringement. This kind of order may only be sought by the author, their rightholder or a licensee.

As a general limit to the possibility to issue such an order, 56a § 2 para prescribes that it can only be issued if the reasons for the measure outweigh the “inconvenience or other harm that the measure would cause the party affected by it or any other opposing interest”.

As a general rule, such orders can only be granted if the claimant submits security (collateral), to prevent frivolous lawsuits from occurring, but the claimant may be exempted if they have limited resources (56c§).

b) Administrative.

There do not appear to exist any administrative measures in Sweden as defined herein.

c) Criminal.

• Financial penalties and imprisonment – sv. böter och fängelsestraff

As a preliminary point, it ought to be noted that infringement of intellectual property rights are regarded in Sweden as criminal in nature because criminal sanctions can be imposed. In particular, the general rule in 53§ para 1 Copyright Act, prescribes a penalty fine or imprisonment (jail) for up to two years for *intentional or grossly negligent* infringement. Criminal sanctions for copyright infringement are therefore only available if a user has acted intentionally or has been grossly negligent. The latter standard is intended to indirectly incentivise the verification of the status quo before engaging in a copyright relevant act.

While criminal liability and sanctions are available for all categories of protected content in general, 53 § 2 para expressly exempts from criminal liability the reproduction of computer programs for own personal non-commercial use, where the original copy that is being reproduced is not used for commercial purposes or in the public sector and the reproduced copy is not made for other purposes than personal use.⁵³⁶ In most cases this will encapsulate computer games.⁵³⁷ The same applies to digital compilations.

Consequently, whereas criminal sanctions might not be available in a limited amount of situations for the unlawful reproduction of computer programs and compilations, the unlawful reproduction of any other protected content and an act of communication of any kind of protected content to the public will always implicate criminal sanctions on condition that the infringer does so intentionally or is grossly negligent.

As to the rules on age limits, the Penal Code prescribes that

1. *The youth of a person who is under 21 years old must be considered when determining the penalty (29 Ch. 7 § 1 para Penal Code). A court may therefore prescribe a shorter imprisonment period, or lower financial penalty, than would otherwise be appropriate for a person who was 21 years old or older.*
2. *Imprisonment (jail) may only be prescribed for a person who is under 18 years old if extraordinary circumstances justify it (30 Ch. 5 § 1 para Penal Code). In any other case, if the court sees imprisonment as the appropriate remedy, such a person is instead put in a young offenders institution.*
3. *No sanction is available for crimes committed by a person under the age of 15 (1 Ch. 6§ Penal Code).*

In 2016 a user (individual) had been sentenced a penalty fine and given a suspended sentence by the Svea Court of Appeals in Case B 1910-15 (judgement delivered on 16 March 2016) for contributory infringement of the communication to the public and reproduction right by having arranged, provided and administered a file-sharing website (www.piratebeirut.com). The website was being hosted on the user's personal computer. Interestingly, in establishing jurisdiction for foreign musical works, the District Court (which the Court of Appeals did not subsequently question) stated laconically that "The authors of the musical works in the albums are nationals in Lebanon and France. These countries are –

⁵³⁶ Hence this no-liability rule will not apply where a person reproduces a computer program at their place of work and brings it home for their own personal use because the original copy is used in business. See Regeringens prop. 1988/89:85, p.17.

⁵³⁷ See *supra* n.512. See also Levin, M., *Lärobok i immaterialrätt*, 11 ed., Norstedts Juridik, 2011, p.558 stating that 53 § 2 para applies to computer games.

and were during the years relevant for the criminal charges – attached to the Berne Convention. This means that copyright has also been available in Sweden”.

Case B 3835-11, Court of Appeals for Western Sweden (judgement delivered on 21 December 2011) concerning download and making available of copyright-protected content through P2P by a 15-year old defendant. The Court found that infringement had taken place owing to the strict liability nature of infringement, however as far as the sanction was concerned, the Court held in relation to downloading that the 15-year old defendant "must have realised" that it was possible that the content was protected by copyright which he could not lawfully download and by proceeding with the download the defendant was grossly negligent. In relation to making the content available, however, the Court held that the defendant "ought to have realised" that the content would be made available as it was being downloaded and concluded that the defendant was not grossly negligent. As the extent of the crimes were limited and where not part of any organised or commercial activity, the Court prescribed the minimum available financial penalty of 1500 SEK (150 EUR).

- Confiscation of property – sv. förverkande av egendom

By virtue of 53a § 1 para Copyright Act property in relation to which a criminal act (pursuant to the Copyright Act) has occurred, or its value or proceeds from the act itself, is declared forfeited, if it is not “obviously unreasonable”. The same applies to remuneration received for costs in connection with the criminal act. Where property has been used as a means to commit a crime, the property may be declared forfeited, if it is necessary to prevent crime or if there are otherwise special reasons for it.

- Seizure of property – sv. beslag av egendom

By virtue of 59§ 3 para Copyright Act, infringing property or property used as means to infringe or intended to be used as means to infringe can be seized where there exists probable cause that a crime has been committed.

This specific measure is only available in criminal matters, although in civil matters claimants may apply for the carrying out of a so-called infringement investigation for the purpose of evidence collection and preservation.

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country’s law against intermediaries to address online copyright infringement by third party users of their services?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

As a preliminary remark it ought to be noted that Swedish law does not provide for any enforcement measures against a party that is not at least secondarily liable for infringement (with the exception an information injunction). In other words, for a measure to be directed to an intermediary, it must be shown that that intermediary has at least in some way contributed to the infringement. To this effect, Swedish copyright law is therefore more stringent than e.g. Art. 8(3) InfoSoc Directive, which does not prima facie require any liability on the part of the intermediary for an injunction to be issued (blocking order).

a) Civil.

- General injunctions, incl. interim injunctions and blocking orders

In relation to general injunctions, the same provisions of the Copyright Act apply for secondary infringement as for primary infringement. Please refer to the answer to Q.7 point a) above.

For the sake of completeness in relation to an intermediary's secondary liability, it ought to be noted that whereas it has been an established practice in Swedish copyright law to determine secondary liability on the basis of the (more stringent) provisions on secondary liability under the Penal Code (*Brottsbalken*), the Swedish Market and Patent Court of Appeals has recently introduced a *civil law definition* of secondary liability. In particular, in Case PMT 11706-15, delivered on 13 February 2017, PMÖD held that section 53b Copyright Act may incorporate "a more passive approach which can be said to influence or contribute to something (...) Even if it is in many cases closer at hand to expect a degree of active behaviour from the person contributing, a type of subordinate behaviour which, in itself, is relatively far from the central event, irrespective of whether it constitutes a contribution within the meaning attributed to it in criminal law or not, is not precluded from still being regarded as contribution in a broader sense"; effectively broadening the scope of secondary liability to what evidently is mere conduit.

- Special injunction ordering the provision of information (information injunction) – sv. informationsföreläggande

In relation to information injunctions, the same provisions of the Copyright Act apply for intermediaries. Please refer to the answer to Q.7 point a) above.

Case law examples:

- NJA 2012 s.975, Sweden Supreme Court (judgement delivered on 21 December 2012), not finding a (potential) information injunction (applied for by rightholders of audio books) ordering the ISP the provision of names and addresses of users of specific IP addresses as violating the e-Privacy Directive (2002/58) nor the Data Retention Directive (2006/24).
- Case PMÖA 660-16, Patent and Market Court of Appeal (judgement delivered on 18 November 2016) obliging an ISP to pay the court costs of a (successful) application for an information injunction concerning names and addresses of users of specific IP addresses.
- Case PMÖÄ 2917-17, Patent and Market Court of Appeals (judgement delivered on 9 April 2018) dismissing foreign claimants' (Copyright Management Services Ltd) application for an information injunction concerning 240 IP-adresses against an ISP and reversing the decision of the first instance court on the ground that CMS had failed to convincingly establish that the ISP was in possession of the information requested in the application. Although the IP addresses were allegedly assigned for the territory of Sweden, the ISP had claimed, following an internal investigation after the judgement of the first instance court, that a significant majority of the IP-addresses in question belonged to other companies, some of which were not operating in Sweden, and some of which belonged to the ISP's foreign subsidiaries. With regards to the latter the court noted (p. 5 of judgement) that a parent company cannot be ordered to provide information held by the subsidiary company.

See also the answer to Question 12 for other examples.

b) Administrative.

There do not appear to exist any administrative measures in Sweden as defined herein

c) Criminal.

- Financial penalties and imprisonment – sv. böter och fängelsestraff

Although 53§ para 1 Copyright Act prescribing a penalty fine or imprisonment for up to two years literally refers to primary liability, secondary liability is encapsulated by virtue of Ch. 23 s. 4(1) of the Swedish Penal Code. By virtue of Ch. 23 s. 4(3) Penal Code, the penalty prescribed will depend on the level of intention and/or negligence attributable to the contributor.

- Confiscation of property – sv. förverkande av egendom

The same applies as for primary infringement.

- Seizure of property – sv. beslag av egendom

The same applies as for primary infringement.

- Criminal sanctions under the Act on Responsibility for Electronic Bulletin Boards

If the provider or operator of a BBS intentionally or with gross negligence fails to remove a message whose posting is an obvious infringement of copyright or neighbouring rights, 7§ 1 para of the Act prescribes a financial penalty or imprisonment for up to six months, or for up to 2 years for a serious crime. For petty offences no sanction is prescribed.

This provision does not however apply if the provider or operator can instead be liable under the Copyright Act.

9. To the best of your knowledge, are there significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

The author is unaware of any specific, relevant, differences between public and private enforcement practices. There is no statutory notice-and-take-down procedure, other than the safe harbour provisions in the E-Commerce Act which require compliance to be applicable. The breadth of the various available (public) means of enforcement permits rightholders to combine public and private enforcement or simply rely on public enforcement. Please see further the answer to Question 12 below.

In so far as ISPs are concerned, because any sanction (except information injunction) requires at least contributory infringement of the addressee, a rightholder will be expected to prove the contributory infringement of the ISP, an accusation that an ISP will most likely be prepared to contest in court. Consequently, there is little incentive for the ISP-industry to develop common codes of conduct relating to notice-and-take-down as a court will need to issue a ruling to justify any act (such as the provision of information about the subscribers).

However, as PMÖD has broadened the definition of secondary liability in civil matters and effectively issued an injunction against an ISP (TPB blocking order), it cannot be ruled out that such codes might develop. To the knowledge of the author no ISPs have voluntarily blocked access to TPB or any other similar website, nor have codes of conduct been developed. Telenor has been reported to voluntarily block access to TPB, however the company is merging with Bredbandsbolaget (the ISP that is the addressee of the only blocking order).⁵³⁸

⁵³⁸ See <https://twitter.com/TelenorSverige/status/996354190552305664>. See also for a detailed description <https://torrentfreak.com/isp-telenor-will-block-the-pirate-bay-in-sweden-without-a-shot-fired-180520/>.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

Yes.

a) If yes, what conditions must be met for that obligation to arise?

Such disclosure is only possible after a judicial court order.⁵³⁹

Please refer to the answer to Question 7 a) “Special injunction ordering the provision of information (information injunction) – sv. informationsföreläggande” for the legal requirements that must be satisfied for such an obligation to arise.

b) If yes, what type of personal data is typically requested?

The list in 53c § 3 para Copyright Act is not exclusive and an applicant may request any information which may be relevant. Typically names and home addresses are requested.

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

This depends on the measure in question. In most cases this will be the author and the rightholder. In the case of general injunctions, information injunctions, infringement investigations, the licensee may also apply for such measures. This is motivated by the belief that licensees may sometimes also be significantly affected by an infringement and their need for information to take measures against infringement is as strong as a rightholder's.⁵⁴⁰

In relation to measures available in criminal matters, it is generally the prosecutor. Swedish law distinguishes between public prosecution (sv. *allmänt åtal*) and private prosecution (sv. *enskilt åtal*), the latter being available only for defamation and insult (5 Ch. 5 § Penal Code). Copyright infringement, as a punishable crime, is categorised as falling under public prosecution (59 § 1 para Copyright Act read together with 20 Ch. 3 § 1 para Penal Code). The initiation of proceedings by a public prosecutor, specifically in relation to copyright infringement, can however only occur if either the aggrieved party has filed a complaint, or prosecution is called for in the public interest (59§ 1 para Copyright Act). However, if the prosecutor decides not to initiate proceedings, private prosecution will be available (20 Ch. 8 § para 1 Penal Code).

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

- Please indicate whether the measures refer to public or private enforcement.

Given the breadth of the information injunction, rightsholders may apply for such an injunction and, having received all the necessary details, threaten with litigation or seek remuneration for specific use which has become known (and hence combine public and private enforcement). One can certainly speculate that a detailed cease and desist letter is more persuasive, and therefore effective, than is a general letter. Whereas the scope of such practices in the past is unknown to the author, it has become more popular recently and taken the form of settlement offers combined with threats of litigation. The

⁵³⁹ Proposition 2008/09:67, p. 145.

⁵⁴⁰ Proposition 2008/09:67, p. 129.

author is unaware of any pending case challenging the substance of these letters, but the contents of the letters certainly have a high deterrence factor.

Please refer to the answer in Question 12-b) below for a detailed account of this practice.

Rights holders have however been rather effective in enforcing their rights against individuals. For example, the following cases (mentioned previously) all concern *primary infringement* by private individuals:

- Case B 3835-11, Court of Appeals for Western Sweden, judgement delivered on 21 December 2011,
- Case B2160-12, Svea Court of Appeals, judgement delivered on 23 April 2011,
- Case B16995-11, Göteborg District Court, judgement delivered on 26 November 2013,
- Case B838-14, Göta Court of Appeals, judgement delivered on 4 April 2014

These cases also show that at least some rightsholders might appear to primarily be interested in putting an end to the infringements, because even though these cases implicated criminal sanctions, the rightsholder did not seek any compensatory award (which is available even if the case has been initiated by a prosecutor).

In a case involving criminal liability for *contributory infringement* (reproduction and communication of sound recordings/musical works to the public through DC++ software), the rightsholder (IFPI Sweden) did not seek a compensatory award.⁵⁴¹ By contrast, in the high profile criminal case concerning The Pirate Bay (also involving contributory infringement), all the rightsholders sought, and were awarded (arguably high) compensatory awards.⁵⁴²

The specific strategy might therefore depend on the specific circumstances, however the use of public means of enforcement can be said to be sufficiently effective and prosecutors are taking on cases involving the “mere” sharing of content (rather than restricting their activity to high-profile, commercial and large scale infringements).

At the time of writing of this report, only one blocking injunction has been granted against an ISP. Although it is expected that blocking injunction applications will increase in the coming years, there has only been one other application, submitted on 25 May 2018, almost 1.5 years after the first blocking injunction was granted. Please see below the answer to point b) for further details.

a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?

In 2017 PMÖD issued the first Swedish injunction ordering an ISP to block their customers’ access to a website (ThePirateBay). Such a development is likely primarily attributable to the CJEU decision in C-314/12 UPC Telekabel v Constantin Film and Wega Filmproduktionsgesellschaft, interpreting inter alia Art. 8(3) InfoSoc Directive, although PMÖD can also be said to have abandoned established case law in deciding on the availability of the injunction (the question of secondary liability). Please refer to the answer in Question 8-a) for information about this particular aspect of the case.

In so far as the information injunction is concerned, which has existed ever since the implementation of the InfoSoc Directive, its application has seemingly increased in popularity during the last three years. It is however difficult to attribute the rise in applications to a single event, other than a simple change in the enforcement strategy.

b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.

⁵⁴¹ Case B 3117-13, Svea Court of Appeals, judgement delivered on 31 October 2013.

⁵⁴² Case nr B 4041-09, Svea Court of Appeals, judgement delivered on 26 November 2010.

Blocking injunctions:

In Case PMT 11706-15 of 13 February 2017, PMÖD issued an injunction against an ISP ordering it to block access to a number of IP and http addresses relating to ThePirateBay (torrents) and Swefilmer (illegal streaming) websites. Although the CJEU decision in *Telekabel* did indicate that such an injunction need not specify the means that the ISP ought to take (and this was indeed one of the alternatives that the rightholders proposed in the case), such a requirement is indeed present in Sweden. In determining the scope of the injunction, PMÖD had firstly underlined that it is not bound by the application submitted by the claimant, and had instead decided to specify the means that the ISP must take, recognising that an injunction was indeed in order. Having regard to the evidence submitted to it, PMÖD firstly noted that the injunction ought not include the blocking of any of the IP addresses as it could not be categorically excluded that they would not be used for other services, and ordered instead the blocking of the general domain names and specific addresses leading to ThePirateBay and Swefilmer websites (DNS blocking). Additionally, and contrary to what the rightholders had wanted, PMÖD imposed a three-year validity period of the injunction.

For the sake of completeness, surprisingly the respondent in the case was only one ISP (arguably the largest), as a result of which the injunction, as a matter of formality, only applies to that ISP. Admittedly the rightholders might have hoped for a domino effect, however some of the remaining ISPs have publicly declared that they will not block access to TPB unless they are forced by a court.

Similarly in a case currently pending before the Patent and Market Court (Case PMT 7262-18), the claimants, most of which are film production companies, also initiated the proceedings against only one ISP (Telia). Three intricacies of this case are especially worth highlighting.

Firstly, in requiring the ISP to cease its own contributory infringement by blocking access to a number of illegal streaming websites (Dreamfilm, Nyafilmer, and Fmovies) and TPB, the claimants have applied for a final injunction as well as a preliminary injunction requiring the immediate stop of such contributory infringement.

Secondly, in requesting the court to grant the injunctions, the claimants list a number of domain names at which the different websites are, or have been, available, but simultaneously argue that the services may register new domain names after an injunction has been granted and that therefore the ISP should be required to take steps to prevent future infringements, effectively therefore requesting an open-ended injunction.

Thirdly, in establishing the existence of primary infringement conducted by the various services to which the ISP is contributing (by allowing its services to be used by the websites when providing internet access to its customers)⁵⁴³, the rightholders are relying on the CJEU's judgement in *Ziggo* for the purpose of establishing liability of TPB on the one hand, but on *GS Media* for the purpose of establishing liability of the streaming websites on the other hand (whereby the infringements take the form of linking to other illegal streaming websites where the content is located) and claiming that the *GS Media* presumption is applicable to those services because of the commercial nature of linking (which the rightholders evidence by reference to the presence of advertising on the relevant websites). Before considering the requested blocking injunction, the court is therefore asked to rule, in so far as the streaming services are concerned and having regard to the Swedish requirements for such injunctions, on whether an ISP is liable for contributory infringement in a situation where the existence of primary infringement is contingent upon the alleged primary infringer's knowledge.

⁵⁴³ Interestingly, the claimants do not simultaneously allege that the ISP's customers infringe any of the rights, neither in relation to TPB nor in relation to the streaming websites. In the first blocking injunction case such an allegation was made only in relation to the customers who used TPB but not to the Swefilmer streaming website. However, not only was the latter service not operating anymore at the time of the proceedings, but it was before the CJEU's judgement in *Filmspeler* (see in particular paras [70]-[71]).

Settlement offer letters and information injunctions

The practice is expected to increase significantly as a result of a number of recent decisions mentioned below. While it is not possible to precisely determine the success of these letters, the law firm handling a number of recent applications for information injunctions and authoring the follow-up settlement offer letters has said that they receive a 60% response rate without however disclosing how many exactly are paying, but noting that legal action will be taken.⁵⁴⁴ In 2017 the Swedish Consumer Protection Agency (Konsumentverket) received approximately 250 requests for advice from individuals who in most cases mistakenly believe such letters to be fake invoices. This has made it possible to obtain detailed information on the content of the letters and some individual responses. Such requests have continued during 2018.

In a striking majority of cases the law firm representing the rightsholders proposes 4500 SEK (450 EUR) to settle a potential copyright claim relating to the downloading (or streaming) and communicating to the public of specific films, usually through P2P networks. The same law firm has also sent settlement offers for alleged downloading and communication to the public on a P2P network of “an erotic film” without specifying the title, offering 7000 SEK as the settlement amount; as well as letters which are speculative in the sense that there is no direct allegation of infringement having been conducted by the addressee but instead contain a statement that a specific film may have been viewed through a service such as Popcorn Time and a request for the provision of information whether the addressee or anyone the addressee may know of (including children) has watched the film in question, combined with an offer to settle the alleged infringement for 4500 SEK. The letters usually specify that the rightsholder is entitled to fair compensation under 54 § Copyright Act⁵⁴⁵ and that such compensation “shall include the [rightsholder’s] costs to trace the infringement and to rectify it”. Interestingly if an individual is taken to court such a case will fall into the category of a small claims case (sv. föräsklat tvistemål)⁵⁴⁶ in which the successful party, in so far as legal costs are concerned, may only be entitled to be reimbursed by the other party for 1 hour of legal advice (per court instance) equivalent in amount to legal advice under the Legal Aid Act (1996:1619) and the court fee⁵⁴⁷.

A non-exhaustive list of recent cases:

- Case nr PMÄ 1937-17, Patent and Market Court, judgement delivered on 10 March 2017. PMD issued an information injunction on application from Copyright Management Services Ltd against an ISP (TeliaSonera), on penalty of 200 000 SEK (ca 20 000 EUR), concerning the provision of names and addresses of its subscribers in relation to ca 5 300 IP addresses, giving the ISP three months to comply.
- Case nr PMÄ 16912-16, Patent and Market Court, judgement delivered on 31 January 2017⁵⁴⁸. PMD issued an information injunction on application from Copyright Management Services Ltd against an ISP (TeliaSonera) on penalty of 200 000 SEK concerning the provision of names and addresses in relation to ca 25 000 IP addresses, giving the ISP 12 months to comply.
- PMÄ 13691-16, Patent and Market Court, judgement delivered on 28 December 2016. PMD issued an injunction on application from Copyright Management Services Ltd against an ISP (TeliaSonera), on penalty of 200 000 SEK, concerning the provision of names and addresses of its subscribers in relation to ca 5600 IP addresses, giving the ISP six weeks to comply. Case

⁵⁴⁴ See <https://www.idg.se/2.1085/1.691043/kravbrev-svenska-fildelare>

⁵⁴⁵ See the answer to Question 7 above for the contents of this section.

⁵⁴⁶ i.e. the value of the claimed amount is under 22 750 SEK for 2018.

⁵⁴⁷ 18 Ch. 8a § Rättegångsbalken (Code of Judicial Procedure). In 2018 the amount equals 1699 SEK (incl. VAT) for legal aid and 900 SEK for the court fee. The remaining costs that the successful party may be reimbursed for in such a case concern exclusively travel costs, witness testimony and translation. In any event the party must evidence the existence of the cost and that it is been reasonably necessary (sv. *skäligen påkallat*) for the protection (enforcement) of the right. Where the party is a larger commercial entity the latter requirement for legal advice will not be satisfied if the case concerns the core activities of the party and is uncomplicated or is recurring in the business (NJA 2007 p. 579, Supreme Court, judgement delivered on 12 September 2007).

⁵⁴⁸ Application for injunction submitted on 28 December 2016. Cf date of judgement in case PMÄ 13691-16 (follows below).

successfully appealed to PMÖD on point concerning time period for submission of information (Case nr PMÖÄ 574-17, Patent and Market Court of Appeal, judgement delivered on 4 May 2017).

- Cases Ä 7496-16, Ä 8275-16, Ä8338-16, Ä 8347-16, Ä 8627-16, Ä 9078-16, Ä 9134-16, Södertörns District Court, judgements delivered 2 September 2016. The district court issued injunctions on application from Crystalis Entertainment and Scanbox Entertainment Distribution respectively against an ISP (TeliaSonera) relating to a total number of ca 8600 IP addresses. Cases successfully appealed to PMÖD on point relating to period for the provision of the information (Cases ÖÄ 8309-16, ÖÄ 8302-16, ÖÄ 8306-16, ÖÄ 8310-16, ÖÄ 8308-16, ÖÄ 8312-16, ÖÄ 8304-16 respectively, Patent and Market Court of Appeals, judgements delivered on 25 January 2017), which PMÖD set to four months.

In determining the reasonable time period within which the ISP must provide the information specified in an information injunction, the courts usually refer to PMÖD's decisions from 25 January 2017 and use the following reference:

- 8600 IP addresses = four months => 2 150 IP addresses = one month

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

Criminal sanctions have been discussed intensively during this time and the Swedish Government has recently appointed an expert to conduct an official enquiry into whether there is a need for increasing criminal sanctions for gross copyright (and trademark) infringements.⁵⁴⁹ The official enquiry is not intended to cover petty infringements or concerning purely private activities, but instead large commercial scale infringements, relating to the use of the internet, counterfeiting etc. The main reason justifying the enquiry is the need to assess whether the current rules ensure effective enforcement of rights and whether they are fit for the type of infringements that are occurring. In particular, the enquiry guidelines state that

*With the help of well-organised sites, the infringements occur quickly, easily and simultaneously openly and anonymously. The sites are directed to a large audience. The activities extend internationally over borders and are conducted commercially, professionally and systematically with the aim to attract new customers and to create substantial revenue for the principals. Not infrequently are the activities linked to bigger actors and serious organised crime. This has resulted in wider infringements which are hard to examine and harmful to rightholders, consumers and the society at large. This can make individual rightholders reluctant to pursue costly civil proceedings. The development indicates that the need of a strengthened legal framework, so that society can act against the most serious crimes, has increased and that the focus ought to be directed towards commercial, organised or strategically planned crime.*⁵⁵⁰

The enquiry report was published in the Official Governmental Reports series (SOU)⁵⁵¹ on 15 February 2018⁵⁵². While noting that in cases dealt by Swedish courts there has not transpired any connection between IP infringement and other gross offences,⁵⁵³ the enquiry essentially proposes the introduction of a new offence - *gross copyright infringement* - into the copyright framework with a

⁵⁴⁹ Kommittédirektiv 2017:4, Straffskalorna för vissa allvarliga immaterialrättsintrång, available at <http://www.regeringen.se/rattsdokument/kommittedirektiv/2017/01/dir.-20174/>

⁵⁵⁰ *ibid.*, p.6-7.

⁵⁵¹ https://en.wikipedia.org/wiki/Statens_offentliga_utredningar

⁵⁵² SOU 2018:6 Utedningen om vissa allvarliga immaterialrättsintrång, *Grovt upphovsrättsbrott och grovt varumärkesbrott*. Available at <https://www.regeringen.se/49191f/contentassets/ec39a402b30e44828089a69516840f16/grovt-upphovsrattsbrott-och-grovt-varumarkesbrott-sou-2018-6.pdf>

⁵⁵³ *ibid.*, p. 44.

minimum prison sentence of six months up to six years⁵⁵⁴, making it equivalent to gross money laundering, gross smuggling offences and gross customs offences. A public consultation has been launched until 5 June 2018.⁵⁵⁵

To my knowledge there have not been any particular widespread debates about the information injunction during this time. It is only recently that the proper “industrial-like” scale of such activities has become known, including the precise steps that rightsholders are taking after obtaining the relevant information. I would expect that this will become an important topic during the coming year.

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions/campaigns aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

- Official:

The Swedish Patent and Registration Office (PRV) and the Swedish Innovation Agency (Vinnova) have since 2016 officially been tasked by the Swedish Government to conduct various types of activities for the benefit of general awareness and public support for the management of intellectual property.⁵⁵⁶

This task involves *inter alia* the organisation of various information and awareness campaigns about copyright infringement with the aim of decreasing copyright infringement in the digital environment and increasing society’s interest to access copyright-protected content through legal alternatives.

As part this effort PRV has created a separate tab on copyright on its own website (<https://www.prv.se/sv/upphovsratt/>) and launched a website in 2018 (<https://www.streamalagligt.se>) aimed to inform the public about copyright generally and streaming in particular. The service is part of Agorateka (www.agorateka.eu) and is supported by the EUIPO. The website is regularly updated with lawful streaming and downloading services for different kinds of content, but it does contain a noticeably wide disclaimer (<https://www.streamalagligt.se/na/en/disclaimer>). The website also includes a number of short films aimed to raise awareness about illegal streaming. Interestingly these films may create the impression that legal streaming is never free of charge, and appear to correlate unlawful streaming services with exorbitant earnings and what appears to be organised criminal activity in the form of counterfeit medicinal products manufacturing.

The films are in English and are available here:

- <https://www.prv.se/sv/upphovsratt/streama-lagligt/film-illegal-streamingverksamhet/>
- See also the following link for a subtitled version (regarding the Swedish text at the end): <https://www.youtube.com/watch?v=aaQZaE2YYBk>

- Non-official:

This author is unaware of any non-official awareness, education and information campaigns originating from the private sector and occurring during the last three years.

The TV and Film Cooperation Committee (whose main aim is to minimise illegal file sharing of films) is managing a website about copyright aimed particularly for school pupils. The webpage includes information about (illegal) streaming.

<http://upphovsratt.nu/>

(please note the use of “ä” in the address and the .nu ccTLD. “Nu” means “now” in Swedish)

⁵⁵⁴ *ibid.*, pp.45-46

⁵⁵⁵ <https://www.regeringen.se/remisser/2018/03/remiss-sou-20186-grovt-upphovsrattsbrott-och-grovt-varumarkesbrott/>

⁵⁵⁶ Decision of the Swedish Government of 17 March 2016, No. N2016/02167/IF, available at https://www.prv.se/globalassets/dokument/om-prv/regeringsuppdrag/regeringsbeslut_n2016_02167_if.pdf

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

N/A

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

These types of studies/data are generally scarce, and neither the rightholders, nor the relevant industry organisations, appear to provide such data. Most of the available data focuses instead on the various means, and scope, of consumption.

The following might however provide some insight into enforcement of online copyright infringement:

Governmental report assessing the legal framework following the implementation of the Enforcement Directive: Helena Jäderblom, *Utvärdering av IPRED-lagstiftningen*, SOU 2012:15 (Official Governmental Report), available at <http://data.riksdagen.se/fil/336D894C-C2B5-4184-9A48-FC9FAD23F940> (available in Swedish). In particular pp. 23-24 (Utvecklingen av brottsmålshanteringen) describe developments in relation to (criminal) case management following the implementation, pp. 25-30 (Tillämpningen av IPRED-lagstiftningen) generally discuss existing case law (incl. provision of some statistics) in relation to the information injunction, evaluate the various legal requirements and other practical aspects, including legal and practical issues related to the injunction.

The Swedish National Council for Crime Prevention (BRÅ) provides statistics on the amount of reported (criminal) copyright infringement (divided into filesharing complaints and non-filesharing complaints). The data is aggregated directly from various enforcement agencies, including the Swedish Police.

Results creation tool (in Swedish only) : <http://statistik.bra.se/solwebb/action/index>

BRÅ's webpage in English: <https://www.bra.se/bra-in-english/home.html>

Data for the last 6 years (total amount of submitted complaints in Sweden):

←

→

↺

🏠

📘

statistik.bra.se/solwebb/action/anmalda/urval/sok

Se utskriftsvänligt format

Öppna som excelfil

Spara som textfil

Anmälda brott

	År							
	2010	2011	2012	2013	2014	2015	2016	2017
	Antal	Antal	Antal	Antal	Antal	Antal	Antal	Antal
Hela landet								
Brott mot upphovsrätten genom fildelning	19	41	40	37	27	34	33	25
Brott mot upphovsrätten ej genom fildelning	55	93	115	80	98	79	378	174

The Swedish National Courts Administration (Domstolsverket) might also be able to provide information about the amount of cases concerning copyright infringement (this information is not

published in the official statistics as the various categories in the statistics are general). Since 2016 the Patent and Market Court (which is in Stockholm) has exclusive jurisdiction for infringement cases, making it easier to directly obtain information and statistics in relation to new cases.

Questionnaire United Kingdom

CHRISTINA ANGELOPOULOS, Lecturer, CIPIL, University of Cambridge

Last updated: 8 June 2018

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded **red**.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.

The main legal instrument in the UK on copyright is the Copyright Designs and Patents Act (CDPA) 1988 (available at: <http://www.legislation.gov.uk/ukpga/1988/48/contents>). The following are also relevant:

- The Copyright and Rights in Databases Regulations 1997 (available at: <http://www.legislation.gov.uk/uksi/1997/3032/contents/made>)
- The Human Rights Act 1998 (available at: <http://www.legislation.gov.uk/ukpga/1998/42/contents>)
- The Electronic Commerce (EC Directive) Regulations 2002 (available at: <http://www.legislation.gov.uk/uksi/2002/2013/contents/made>)
- The Communications Act 2003 (esp. ss. 124A-124N, added with amendments introduced by the Digital Economy Act 2010, see below) (available at: <http://www.legislation.gov.uk/ukpga/2003/21/contents>)
- The Intellectual Property (Enforcement, etc.) Regulations 2006, ss. 1-5 (available at: <http://www.legislation.gov.uk/uksi/2006/1028/contents/made>)
- The Digital Economy Act 2010 (available at: <http://www.legislation.gov.uk/ukpga/2010/24/contents>)

2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?

UK law not employ the term ‘intermediary’ *per se*. Instead, the Electronic Commerce (EC Directive) Regulations 2002 use the term ‘information society service provider’. This is an obvious loan from the E-Commerce Directive (2000/31/EC). Section 2(1) of the Regulations defines the term as follows:

- A 'service provider' is 'any person providing an information society service'.
- 'Information society services' cover 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service'. For a more detailed definition, the section refers to Article 2(a) and Recital 17 of the E-Commerce Directive.

In addition to the above, ss. 17-19 of the same Regulations transpose the safe harbour provisions (immunities) of Articles 12-14 of the E-Commerce Directive. These are available to three types of providers: the providers of 'mere conduit' services, the providers of 'caching' services and the providers of 'hosting' services. The relevant services are defined as follows:

- According to s. 17, a 'mere conduit' service is an information society service 'which consists of the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network'.
- According to s. 18, a 'caching' service is an information society service 'which consists of the transmission in a communication network of information provided by a recipient of the service [where] the information is the subject of automatic, intermediate and temporary storage [and] that storage is for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request.'
- According to s. 19, a 'hosting' service is an information society service 'which consists of the storage of information provided by a recipient of the service'.

3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
- Depends on the commercial or for-profit nature or intent of the use or user;
- Is uncertain and, if so, why;
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

a) **Downloading copyright-protected content from illegal/unauthorized sources on the Internet.**

Downloading copyright-protected content in the UK would qualify as an act of reproduction. The reproduction of a work is an exclusive right of the copyright holder according to ss. 16-17 of the CDPA. As a result, if done without the authorisation of the copyright-holder, downloading protected content will infringe copyright.

The above has been confirmed by case law. The leading case in this regard is *Twentieth Century Fox Film Corporation v Newzbin* [2010] EWHC 608. According to *Newzbin* (see para. 97), the premium members of the Usenet indexer Newzbin, by making use of the facilities this provided to download copies of copyright-protected films, had infringed copyright. Likewise, in *Dramatico Entertainment v British Sky Broadcasting* ([2012] EWHC 268) (*Dramatico v Sky (No.2)*), the court found that the users of the BitTorrent file-indexer The Pirate Bay who select a torrent file in order to obtain a copy of particular piece of content and then download the associated content files copy the content contained in those files on their computer (see para. 40-43).

The relevant liability does not appear to depend on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content or on the for-profit nature or intent of the use or user. It also does not depend on the type of protected content.

b) Streaming copyright-protected content from illegal/unauthorized sources on the Internet.

There have been a number of decisions on streaming websites in the UK. These have arisen in the context of proceedings for the grant of an injunction against Internet service providers ordering them to block access to streaming websites under s. 97A CDPA. According to standing case law (see *Dramatico v Sky* [2012] E.C.D.R. 24 at [4]), a condition for the grant of such an injunction is that the users and/or the operators of the site whose blocking is sought be shown to have infringed the claimants' copyrights. It has therefore become necessary to consider whether either the streaming websites themselves or their users infringe copyright.

The first such decision to be handed down by the British courts was *FAPL v Sky (The Football Association Premier League v British Sky Broadcasting)* [2013] EWHC 2058 (Ch) (16 July 2013). This concerned FirstRow, a website which operates as an indexing and aggregation portal to streamed broadcasts of sporting events. The court made clear that the streams that are indexed on FirstRow are provided by third party streamers using one of a number of User Generated Content (UGC) websites and that FirstRow did not itself transmit any of the streams. Rather, the streams emanated from the UGC sites and were embedded into FirstRow, so that the streams were listed as links on FirstRow's website.

The court concluded that FirstRow, by aggregating a large number of streams from a variety of streamers, indexing them for the convenience of the user and providing a simple link for the user to click on in order to access a specific stream was communicating works to the public. The court also found that, even if it was mistaken about this, the UGC sites themselves certainly communicate the works to the public and that the operators of FirstRow were jointly liable for this. The court did not consider whether the UGC sites might qualify for the hosting safe harbour. Finally, the court found that publicans who use FirstRow to screen Premier League matches in their public houses are also communicating FAPL's copyright works to the public.

Subsequently, two further s. 97A injunctions have been issued that are relevant to streaming. *Paramount v Sky (No. 1) (Paramount Home Entertainment International v British Sky Broadcasting)* [2013] EWHC 3479 (Ch) concerned a blocking request against streaming websites SolarMovie and TubePlus. Again, it was found that neither of these hosted the content that was streamed. Instead, they ensured that it was comprehensively categorised, referenced, moderated and searchable. The court found that both SolarMovie and TubePlus and the third party websites that hosted the content were communicating protected works to the public. SolarMovie and TubePlus were also found to be jointly liable for the communication to the public done by the host websites. In addition, it was also found that the users who upload protected content to the host sites and provide SolarMovie and TubePlus with links to that content were communicating protected works to the public.

More recently, in March 2017, s. 97A CDPA injunctions were also granted for the 'live' blocking of access to infringing streams of Premier League footage to UK consumers (see *Football Association Premier League v British Telecommunications* [2017] EWHC 480 (Ch) (*FAPL v BT*)). In this case, the injunctions were directed at the actual streaming servers. 'Live' blocking only has effect during the time period when the relevant content is being streamed, i.e. at the times when live Premier League match footage is being broadcast.

It was held that users who access a stream of a protected work cause their computer, mobile device or set-top box to create copies of that work in the memory of those devices. In some cases, a substantial part of a work may be copied in a single frame (for example, a logo). In the case of films or matches, copying of a substantial part is very likely to occur if users stream footage of any appreciable segment

of the match. The operators of target servers which stream protected works were also found to: a) be communicating the works to the public; b) have authorised copying by their UK users; and c) act as joint tortfeasors in relation to the infringements of those users.

The court did not appear to consider whether the reproductions made by users streaming the content would be eligible for the defense of s. 28A CDPA on temporary copying. This omission should be taken to be confirmed as unproblematic by the CJEU's recent judgement in *Filmpeleer* (Case C-527/15). Here, the CJEU found that acts of temporary reproduction on a multimedia player of a copyright-protected work obtained by streaming from a website belonging to a third party offering that work without the consent of the copyright holder do not satisfy the conditions of the temporary copying exception. Presumably, the same conclusion would hold true of copies made in the memory of other devices as well.

The above decisions appear to confirm that the following acts related to streaming will amount to a communication to the public:

- The hosting of streams of protected content;
- The aggregation of a large number of such streams from a variety of streamers, indexing them for the convenience of the user and providing a simple link for the user to click on in order to access a specific stream;
- The screening of such streams in a public place;
- The uploading of protected content for the purposes of streaming;
- The provision of links to unauthorised streams of protected content.

If done without the consent of the right-holder, these acts will thus constitute copyright infringement.

In addition, the accessing of a stream of a protected work by an end-user will amount to an act of reproduction. Again, if done without the consent of the right-holder this will constitute a copyright infringement.

Finally, the aggregation of a large number of streams of protected content from a variety of streamers, indexing them for the convenience of the user and providing a simple link for the user to click on in order to access a specific stream will also result in liability for joint tortfeasance in another's primary infringement. The provision of streaming servers will also lead to liability for authorising the unlawful copying of end-users and as a joint tortfeasor in relation to that copying.

Whether or not knowledge or awareness are relevant to liability for any of the above acts is at the moment uncertain. Notably, the infringement of a copyright holder's exclusive right has traditionally been understood to be a strict liability tort in the UK. However, the above judgements do appear to take subjective elements into account, at least with regard to the liability of the aggregator sites. So, for example, in *FAPL v Sky*, the High Court observed that First Row employed moderators who vet and index the submissions made by third party streamers (see para. 15). Moreover, whilst it gave the impression, by way of a 'submit your video' link, that it was open to the submission of streams by any member of the public, according to the court, in reality its submissions were instead sourced from a number of existing, trusted streamers. Similarly, in *Paramount v Sky (No. 1)*, the court explained that SolarMovie used moderators to approve links to content that were supplied by registered users. The court noted that it was not clear to what extent links on TubePlus were provided by users and to what extent by the operators of the website. Both sites were described as 'ensuring that the content is comprehensively categorised, referenced, moderated and searchable' (see para. 5). A certain degree of knowledge could be said to be inherent to all these acts.

In any event, liability for joint tortfeasance, as well as for the authorisation of another's infringement will certainly take subjective elements into account. For joint tortfeasance, these would be the inducement or procurement of the infringement or the joining in a common design with the primary

infringer pursuant to which an infringement is committed.⁵⁵⁷ Authorisation has been interpreted by the UK courts as meaning ‘to sanction, countenance or approve’ or ‘to grant or purport to grant to a third party the right to do an act.’⁵⁵⁸ In both cases, knowledge or awareness might be relevant.

Further than this, the liability of users who provide links to streamed content is likely to depend both on knowledge and awareness and the for-profit nature or intent of the use or user. Although there was a considerable amount of uncertainty on this issue at the time that these decisions were handed down (something reflected in the language used by the courts, which treated hyperlinking and uploading as coming together to support the liability of end-users, see *Paramount v Sky (No. 1)*, para. 37), the recent case law of the CJEU on hyperlinking will presumably be taken into account in the future.

It does not appear that knowledge or awareness are relevant to any of the other acts listed above that might attract liability in relation to streaming.

Liability for streaming in the UK does not appear to depend on the type of protected content or on the for-profit nature or intent of the use or user.

c) Stream-ripping copyright-protected content.

I am not aware of any court decisions to date in the UK on stream-ripping copyright-protected content. However, a consistent application of the principles that can be derived from the case law on downloading mentioned above would lead to the conclusion that the reproduction right would be infringed by stream-ripping.

It is unclear whether stream-ripping infringes the rules on the legal protection of technological measures. This would be a possibility only if the ripped content is protected by TPMs. But even in that case, the terms and conditions of the relevant online service would probably regulate whether this type of use is permitted or prohibited. If prohibited, the reasoning of the previous paragraph applies, leading to the conclusion that the reproduction right would be infringed by stream-ripping.

d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.

Uploading copyright-protected content in the UK would qualify as an act of communication to the public. The communication of the work to the public is an exclusive right of the copyright holder according to ss. 16 and 20 of the CDPA. As a result, if done without the authorisation of the copyright-holder, uploading protected content will infringe copyright.

The leading case in this regard is the aforementioned *Dramatico v Sky (No.2)*. This concluded that the users of The Pirate Bay who allow copies of works on their computers to be uploaded to the ‘swarm’ are communicating them to the public (see para. 68-71). Subsequent decisions have confirmed this conclusion. For example, as mentioned above, *Paramount v Sky (No. 1)* found that users who upload protected content to the host sites for the purposes of streaming are communicating works to the public (see para. 37).

Presumably, uploading copyright-protected content should also be taken to qualify as an act of reproduction. This is suggested, for example, by leading textbook Bently & Sherman.⁵⁵⁹ To my knowledge however, nothing to this effect has been mentioned in the relevant case law. Presumably, this is because most of that case law has focused on peer-to-peer technology, which by its nature makes it difficult to distinguish between acts of downloading and uploading (on this see *Dramatico*

⁵⁵⁷ L. Bently and B. Sherman, *Intellectual Property Law* (4th edition, OUP), pp. 1208-1210.

⁵⁵⁸ *Ibid.*, p. 171.

⁵⁵⁹ *Ibid.*, pp. 144 and 147.

(No. 2) (at para. 68). Where technology, however, is used that makes such a distinction meaningful, consideration of the reproduction right for uploaders would likely follow.

The relevant liability does not appear to depend on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content or on the for-profit nature or intent of the use or user. It also does not depend on the type of protected content.

e) Posting hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.

There has been no case law to date in the UK on hyperlinking and copyright. Having said this, the assumption must be that – as long as the UK remains within the single market – domestic courts are bound by the case law of the CJEU. As a result, the conclusions of the CJEU in *GS Media* (Case C-160/15) must be assumed to apply in the UK. Hyperlinking to copyright-protected content that has been made available online without the express authorisation of the right-holder should therefore be considered to amount to a communication to the public under UK law, as long as the poster of the hyperlink knew or ought to have known that the hyperlink provides access to a work illegally placed on the Internet, for example owing to the fact that he was notified thereof by the copyright holders. If the posting of hyperlinks is carried out for profit, then a rebuttable presumption of knowledge applies.

Since *GS Media*, there has only been one case to date where the issue of hyperlinking was touched upon (although in passing) by a UK court. In the aforementioned *FAPL v BT* case, the judge stated that, where the operators of the target servers link to freely available sources of Premier League footage, the evidence indicated that they did so for profit, frequently in the form of advertising revenue (para. 37). Thus, in application of *GS Media*, they were presumed to have the requisite knowledge for the communication to be to a new public.

Liability for hyperlinking in the UK does not appear to depend on the type of protected content.

- Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard surface hyperlink, deep-link, embedded or framing hyperlink).

The case law of the CJEU does not appear to make a distinction in this regard (see Cases C-466/12, *Svensson*, C-348/13, *BestWater* and C-160/15, *GS Media*). Therefore, although to my knowledge there has not been any case law on this in the UK, it must be assumed that UK courts would not do so either.

f) The sale of Kodi boxes or similar devices.

There has been no case law to date in the UK on Kodi boxes or similar devices. As above however, it must be assumed that, as long as the UK remains within the single market, domestic courts are bound by the case law of the CJEU. As a result, the conclusions of the CJEU in *Filmspeler* (Case C-527/15) must be assumed to apply to the UK. The sale of Kodi boxes or similar devices should therefore be considered to amount to a communication to the public under UK law, if add-ons have been pre-installed on them that contain hyperlinks to websites that are freely accessible to the public on which copyright-protected works have been made available to the public without the consent of the right-holders.

It is worth noting that, as mentioned above, the blocking order against streaming servers that was issued in *FAPL v BT* was justified by the judge by reference to the fact that consumers are increasingly turning to set-top boxes, media players and mobile device apps to access infringing streams, rather than web browsers running on computers. According to the court, this means that ‘traditional blocking orders (targeting websites) will not be able to prevent the growing majority of infringements, because these devices do not rely upon access to a specific website in order to enable

consumers to access infringing material. Instead, such devices can connect directly to streaming servers via their IP addresses' (see para. 11-16).

g) Other types of unauthorized online use of copyright-protected content not listed above.

Injunctions have also been issued in the UK against Internet service providers (ISPs) ordering the blocking of websites that make available for download 'Popcorn Time', an open source application which can be downloaded by the user onto their computer and which enables the user to obtain film and TV content using the BitTorrent protocol. The application operates as a BitTorrent client, but with the addition of integrated media player software, an index/catalogue of titles and images and descriptions of titles. The High Court refused to find that the operators of websites that make Popcorn Time available for download (Popcorn Time application source or PTAS websites) communicate works to the public. The judge concluded that it is the application itself which intervenes to make the films available, not the websites. Authorisation was also denied in that case, although joint tortfeasance was established. The same outcome was reached with regard to so-called SUI websites, i.e. the source of a data file with the index/catalogue which is to be presented to the user when they run the Popcorn Time application. See *Popcorn Time* [2015] EWHC 1082 (Ch), para. 31-56.

From this outcome we can conclude that subjective elements are relevant to the liability of such websites (as is the rule in cases of joint tortfeasance, see above). However, the type of protected content and the for-profit nature or intent or the use or user would not be.

We can presume from the judge's reasoning that 'Popcorn Time'-style applications would themselves be found to be communicating works to the public in the UK.

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

Not as far as I am aware.

Section 97(1) CDPA does state that where 'in an action for infringement of copyright it is shown that at the time of the infringement the defendant did not know, and had no reason to believe, that copyright subsisted in the work to which the action relates, the plaintiff is not entitled to damages against him, but without prejudice to any other remedy.' It is perhaps possible that this provision might be employed in cases involving child-infringers to exclude an award of damages. I am not however aware of a case that has considered the matter.

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country's law? If yes, please cite and/or describe as completely as possible the scope of the exemptions or safe-harbors.

Yes. As mentioned above, Articles 12-14 of the E-Commerce Directive have been implemented into UK law through ss. 17-19 of the Electronic Commerce (EC Directive) Regulations 2002. The transposition is almost word-to-word. As a result, the conditions are identical. The only difference is the elimination of the final paragraph of each safe harbour that states that it shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement. Instead, the British implementation clarifies that the safe harbours protect the service providers from any liability that might otherwise apply for damages or for any other pecuniary remedy or for any criminal sanction. This amounts to an interpretation of the Directive's provisions for the purposes of their clear application in the context of British law.

No other liability exemptions or safe harbours exist.

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbours? If yes, please cite and/or describe as completely as possible the relevant differences.

There has been very limited case law in the UK on the safe harbours. One question which has arisen is the same one that is widely discussed in the EU context at the moment, i.e. whether modern Web 2.0 platforms that store copyright-protected works that have been uploaded by their users in a public manner can be said to qualify for the protection of the hosting safe harbour. The issue turns on the interpretation of the condition of a 'neutral role', as that has been introduced by the case law of the CJEU on the basis of Recital 42 of the E-Commerce Directive (see Joined Cases C-236/08 to C-238/08, *Google France v Louis Vuitton*, para. 112-120 and Case C-324/09, *L'Oréal v eBay*, para. 112-117). While both relevant cases were trade mark ones, the conclusions drawn by the CJEU on Article 14 of the E-Commerce Directive are relevant for the purposes of copyright as well. According to the CJEU, an activity will be 'neutral' where it is 'of a mere technical, automatic and passive nature, so that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored'. This will be the case, for example, where the provider stores information on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers. By contrast, a provider will play an active role where, for example, it has provided assistance which entails, in particular, optimizing, promoting or drafting the information.

L'Oréal v eBay, the second of the two cases, came out of the British courts ([2009] EWHC 1094). It was however ultimately settled out of court in 2014. As a result, it is not currently possible to say whether eBay – and, with it, similar platforms more relevant for copyright – would be seen as qualifying for the hosting safe harbour in the UK.

In a more recent case known as *Fanatix (England And Wales Cricket Board Ltd & Anor v Tixdaq Ltd & Anor* [2016] EWHC 575), the High Court considered the liability of the operators of a Vine-inspired mobile application which allowed users to upload and add commentary to screen-captured 8-second clips of broadcast footage. The question arose whether the operators were protected by the safe harbours. The application of the mere conduit safe harbour was rejected by the judge, as the defendants' service did not merely involve the transmission of information, but also storage. No final conclusion was reached with regard to the hosting safe harbour. However, based on *L'Oréal v eBay*, the judge did offer the provisional view that this defence would only be available in respect of user-posted clips which were not editorially reviewed by the defendants, but not in respect of clips which were editorially reviewed.

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:

- The suspension from the Internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.

- The monitoring or **filtering** of content.
- The **blocking** and removing of infringing content, including notice-and-takedown.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- **Graduated response systems.**

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

Chapter VI of Part I of the CDPA 1998 is dedicated to the remedies that a claimant may obtain for the infringement of their copyright. According to s. 96(2) CDPA, in an action for infringement of copyright all relief by way of damages, injunctions, accounts or otherwise is available to the plaintiff as is available in respect of the infringement of any other property right.

According to s. 97(1), where in an action for infringement of copyright it is shown that at the time of the infringement the defendant did not know and had no reason to believe, that copyright subsisted in the work to which the action relates, the plaintiff is not entitled to damages against him, but without prejudice to any other remedy. At the same time, according to s. 97(2), additional damages might be ordered where the circumstances of the case require it, having particular regard to: (a) the flagrancy of the infringement; and (b) any benefit accruing to the defendant by reason of the infringement.

Claimants might opt for an account of profits instead of claiming damages. This is an equitable remedy that deprives the defendant of any profits made as a result of their infringement. It cannot be claimed in addition to damages and is discretionary, so may be refused by the court.⁵⁶⁰

Injunctions may be both interim and final. A final injunction will usually be granted to copyright owners who prove at trial that their rights have been infringed by the defendant. However, it must be kept in mind that the injunction is an equitable remedy in origin and thus is discretionary and might be refused.⁵⁶¹

Interim injunctions are granted if the matter is urgent or if it is otherwise desirable in the interests of justice. In intellectual property cases, including therefore copyright cases, as a general rule applications for interim injunctions are assessed according to the approach set out by the House of Lords in *American Cyanamid v Ethicon* ([1975] AC 396). This requires that the court first assess whether there is 'a serious question to be tried'. If the court decides that this threshold has been passed, it then goes on to consider whether it would be fair that the injunction be granted. Three factors are taken into account in this regard: whether damages would be an adequate remedy, the balance of convenience and the merits of the parties' cases.⁵⁶²

⁵⁶⁰ L. Bently and B. Sherman, *Intellectual Property Law* (4th edition, OUP), p. 1261.

⁵⁶¹ *Ibid.*, p. 1250.

⁵⁶² *Ibid.*, pp. 1238-1246.

To enable copyright-holders to preserve evidence prior to trial, the English courts developed the so-called '*Anton Piller* order'.⁵⁶³ This has now been renamed 'search order'.⁵⁶⁴ A search order permits a claimant to inspect the defendant's premises and to seize or copy any information that is relevant to the alleged infringement. Before an order is granted, the claimant must show that there is an extremely strong case on its face and that the potential damage would be very serious. The claimant must also show that the defendant has incriminating material in their possession and that there is a real possibility that the evidence will be destroyed.⁵⁶⁵

The application for a search order may be combined with a so-called 'freezing order' or 'asset preservation order' (formerly known as a '*Mareva* injunction').⁵⁶⁶ This can be used to order the retention of property pending the outcome of litigation.

Other available remedies, such as delivery up (see s. 99 CDPA) and the right to seize infringing copies (s. 100 CDPA) require tangible copies of protected works and are therefore not usually relevant to online infringement.

b) Administrative.

In April 2010, the Digital Economy Act 2010 was adopted (not to be confused with the Digital Economy Act 2017). This was intended to introduce a so-called 'three strikes and you're out' or 'graduated response' system for the online enforcement of copyright. The idea was to oblige Internet service providers to police the activities of their subscribers by sending them notices in cases where a report was made by a copyright owner that connected the subscriber's IP address with a copyright infringement (s. 3 DEA 2010). If a subscriber was sent a certain number of notifications, they were to be added to a 'copyright infringement list' that would be made available to copyright owners, who could then take action against them (s. 4 DEA 2010). For this purpose, Ofcom, the communications industry regulator, was to establish an 'obligations code', governing when and how an intermediary would send notifications to subscribers and when these notifications would result in the disconnection of an infringing subscriber (s. 5-7 DEA 2010).

An application for the judicial review of the Act (including on the basis of incompatibility with the E-Commerce Directive) was unsuccessful.⁵⁶⁷ Nevertheless, the system remains controversial and has yet to be brought into operation. The UK government has in the meantime indicated its preference for a voluntary scheme.⁵⁶⁸ Such a scheme, known as VCAP or the Voluntary Copyright Alert Programme, was agreed upon in July 2014 between the film and music industry and four large ISPs (BT, Virgin, Sky and TalkTalk). The system forms part of the industry-led scheme Creative Content UK (CCUK) (see below). It is modelled on the 'copyright alert system' that was introduced earlier in the US.

The VCAP scheme involves agents of copyright owners sending evidence of copyright infringement to ISPs, which then send letters or 'alerts' to infringing customers. The letters are not directed at specific individuals, as it is recognised that a single IP address may be used by several people. The letters are designed to discourage infringement, without carrying legal sanctions. Only four letters can be sent to an address associated with a particular IP address. Each letter will use language escalating in severity. Although following the fourth and final alert, no further action can be taken under the Programme, VCAP will not prevent copyright owners from pursuing legal action against individuals for copyright infringement. The government has also warned that if VCAP fails to reduce illegal downloading significantly, it will implement stricter measures.⁵⁶⁹

⁵⁶³ *Anton Piller v Manufacturing Processes* [1976] Ch 55.

⁵⁶⁴ Civil Procedure Act (CPA) 1997, s. 7; Civil Procedure Rules (CPR) Practice Direction 25A.

⁵⁶⁵ L. Bently and B. Sherman, *Intellectual Property Law* (4th edition, OUP), p. 1216.

⁵⁶⁶ CPR, r. 25.1(1)(f).

⁵⁶⁷ See: *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills* [2011] EWHC 1021.

⁵⁶⁸ L. Bently and B. Sherman, *Intellectual Property Law* (4th edition, OUP), p. 1215.

⁵⁶⁹ For more information, see: https://wiki.openrightsgroup.org/wiki/Voluntary_copyright_alert_programme.

The first copyright ‘alerts’ were sent to subscribers in January 2017.⁵⁷⁰

c) Criminal.

Sections 107-110 CDPA 1998 deal with criminal liability for copyright infringement. A variety of different acts of primary copyright infringement are covered by these provisions. For the purposes of online infringement, most pertinent is s. 107(2A) CDPA. This was amended very recently with the Digital Economy Act 2017.

According to s. 107(2A) CDPA, a person who infringes copyright in a work by communicating it to the public commits an offence, if that person: (a) knows or has reason to believe that they are infringing copyright in the work; and (b) either

- (i) intends to make a gain for themselves or another person, or
- (ii) knows or has reason to believe that communicating the work to the public will cause loss to the owner of the copyright, or will expose the owner of the copyright to a risk of loss.

According to s. 107(2B) CDPA, ‘gain’ and ‘loss’ extend only to gain or loss in money and include any such gain or loss whether temporary or permanent. Loss includes a loss by not getting what one might get.

According to s. 107(4A) CDPA, a person guilty of such an offence is liable: (a) on summary conviction to imprisonment for a term not exceeding three months or a fine or both; (b) on conviction on indictment to a fine or imprisonment for a term not exceeding ten years or both.

According to s. 109 CDPA, search orders may also be available where a justice of the peace (or, in Scotland, a sheriff or justice of the peace) is satisfied by information on oath given by a constable (or, in Scotland, by evidence on oath) that there are reasonable grounds for believing: (a) that an offence under s. 107(2A) CDPA has been or is about to be committed in any premises; and (b) that evidence that such an offence has been or is about to be committed is in those premises.

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country’s law against intermediaries to address online copyright infringement by third party users of their services?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

Section 97A CDPA implements into UK law Article 8(3) of the InfoSoc Directive. According to this, the High Court (in Scotland, the Court of Session) shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright. In determining whether a service provider has actual knowledge for the purpose of this section, a court shall take into account all matters which appear to it in the particular circumstances to be relevant, including:

- (a) whether a service provider has received a notice through a means of contact made available in accordance with regulation 6(1)(c) of the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013); and

⁵⁷⁰ ISP Review, ‘UPDATE2 UK ISPs to Send First Internet Piracy Warning Letters this Month’, 10 January 2017, available at: <http://www.ispreview.co.uk/index.php/2017/01/big-uk-isps-send-first-internet-piracy-warning-letters-month.html>.

- (b) the extent to which any notice includes (i) the full name and address of the sender of the notice; (ii) details of the infringement in question.

Most of the case law applying s. 97A CDPA has concerned blocking injunctions. In that case law, the courts have interpreted s. 97A CDPA as requiring the fulfilment of four conditions before a blocking injunction can be issued: (a) the defendants must be service providers; (b) the users and/or the operators of the websites targeted for blocking must infringe the claimant's copyrights; (c) the users and/or the operators of the websites targeted for blocking must use the defendants' services to do that; (d) the defendants must have actual knowledge of this fact.

In addition to the above, intermediaries might also be subject to the so-called *Norwich Pharmacal* order (NPO).⁵⁷¹ This is a form of disclosure order, made under the equitable jurisdiction of the court. An NPO is typically obtained where a party knows that wrongdoing has taken place against it, does not know the identity of the wrongdoer and can identify a third party who has this information. In 2012, a *Norwich Pharmacal* order was issued in a copyright case, *Golden Eye & Ors v Telefonica UK* [2012] EWHC 723 (Ch) against an ISP for the purpose of disclosure of identifying information on its infringing subscribers. The case concerned the unauthorised peer-to-peer file-sharing of pornographic films. Consumer Focus, a consumer watchdog, intervened on behalf of the affected subscribers.

In its judgment, the High Court followed the lead set by the CJEU in *Promusicae* (Case C-272/06) and applied an "ultimate balancing test" for the resolution of the dispute. To this end, the justifications for interfering with or restricting each of two conflicting rights were considered: on the one hand the copyright-holders' right to their property and on the other hand the subscribers' right to the protection of their privacy and personal data. With regard to the first, the substantial scale of the infringement of the claimants' copyrights was noted, as well as the obvious necessity of the communication of the names and addresses of the end-users involved. With regard to the second, the judge observed that the end-users were ordinary consumers, likely on a low income and without ready access to specialised legal advice; that the order sought would by definition invade their privacy and impinge upon their data protection rights; that, due to inevitable errors, they may not be guilty of infringement at all and that the subject matter of the claim (which involved accusations of unauthorised use of pornographic material) was likely to cause embarrassment.

On this basis, the judge opted to grant the order, but concluded that the precise terms of the letter to be sent to end-users were significant. The judge objected to the draft letter submitted before him as, although it took sufficient account of the interests of both the claimant and the ISP, it did not account for the rights of the users themselves, being misleading, one-sided, occasionally incorrect and excessively demanding in terms of the time-frame it established for responses. Additionally, the letter contained a threat of disconnection or of a slowing-down of Internet speeds that was unjustified in the circumstances. Finally, it requested the payment of an arbitrary figure of £700 that was insupportable. As an alternative, the judge endorsed the case-by-case approach, finding that a settlement sum should be individually negotiated with each end-user. The judge also recommended as a safeguard against abuse the selection of a suitable set of "test cases" that could investigate common issues that are likely to arise.

Finally, the judge limited the scope of the order to only two of the claimants, as the claims of the rest were based on agreements for the aggregation of disclosure rights in return for a share in recoveries. According to the judge, this "would be tantamount to the court sanctioning the sale of the [subscribers'] privacy and data protection rights to the highest bidder." The Court of Appeal later

⁵⁷¹ A *Norwich Pharmacal* order was first granted in 1974 by the House of Lords in *Norwich Pharmacal Co. v Customs and Excise Commissioners* [1973] UKHL 6 (26 June 1973). For more on *Norwich Pharmacal* orders, see S Sime, *A Practical Approach to Civil Procedure* (18th ed., Oxford University Press 2015) 496-506 and P Matthews & H M Malek, *Disclosure* (4th ed., Sweet & Maxwell 2012) 63-100. On their application to Internet intermediaries in intellectual property cases, see L. Bently and B. Sherman, *Intellectual Property Law* (4th edition, OUP), p. 1213 and C. Angelopoulos, *European Intermediary Liability in Copyright* (Wolters Kluwer, 2016), p. 183-185.

overturned this restriction (see *Golden Eye (International) Ltd & Ors v Telefónica UK Ltd & Anor* [2012] EWCA Civ 1740).

b) Administrative.

The information provided above in the answer to Q.7(b) is also relevant to intermediaries, to the extent that their services are enlisted to send notices to end-users. Other than that, I don't know of any administrative enforcement measures, procedures, remedies or sanctions that are available in the UK directly against intermediaries.

c) Criminal.

I am not aware of any criminal measures, procedures, remedies or sanctions that are available against intermediaries *per se* in the UK. Of course, intermediaries will be criminally liable in the same way as any other infringer where they commit the offense of s. 107(2A) CDPA, mentioned in the answer to Q.7(c) above.

They might also be found to have committed a criminal offense, if they are found to have made an article specifically designed or adapted for making copies of a particular copyright work or have such an article in their possession, knowing or having reason to believe that it is to be used to make infringing copies for sale or hire or for use in the course of a business (on this see s. 107(2) CPDA). In this case, in accordance with s. 107(5) CDPA, they will be liable on summary conviction to imprisonment for a term not exceeding three months or a fine not exceeding level 5 on the standard scale,⁵⁷² or both.

It is theoretically possible that an intermediary may also be found secondarily liable for a primary offender's acts under s. 8 of the Accessories and Abettors Act 1861. This provides that criminal sanctions may be imposed upon those who 'aid, abet, counsel or procure' the commission of an offence. This could result in liability for those who 'aid, abet, counsel or procure' the offense of s. 107(2A) CDPA. To date however I am not aware of any case where this option has in fact been considered.⁵⁷³

9. To the best of your knowledge, are there significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

Not as far as I am aware.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

a) If yes, what conditions must be met for that obligation to arise?

b) If yes, what type of personal data is typically requested?

Online intermediaries may be ordered by the courts to disclose the personal data of individuals involved in copyright infringing activities to rights holders. For further details on this, see *Norwich Pharmacal* orders (NPOs), discussed above.

⁵⁷² On the standard scale, see Sec. 37 of the Criminal Justice Act 1982.

⁵⁷³ For more on this possibility please see P. Davies, 'Accessory Liability: Protecting Intellectual Property Rights' (2011) 4 IPQ, p. 390-409.

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

According to s. 96 CDPA, an infringement of copyright is actionable by the copyright owner. According to s. 101(1) CDPA, an exclusive licensee also has (except against the copyright owner) the same rights and remedies in respect of matters occurring after the grant of the licence as if the licence had been an assignment (i.e. as if the licensee were the copyright holder). According to s. 101A CDPA, a non-exclusive licensee may also bring an action for infringement of copyright, if: (a) the infringing act was directly connected to a prior licensed act of the licensee; and (b) the licence is in writing and is signed by or on behalf of the copyright owner and expressly grants the non-exclusive licensee a right of action under this section.

Section 97A CDPA does not make any reference to who may apply for an injunction against service providers whose services are used by others to infringe copyright. Nevertheless, as mentioned above, one of the conditions developed by the courts for the grant of such an injunction is that the users and/or the operators of the targeted websites must infringe the claimant's copyrights. This would suggest that the applicants must be the owners of the copyright whose infringement is alleged. Having said that, in other cases the third condition has been rephrased to simply require that 'the users and/or operators of the target websites infringe copyright', without specifying to whom this copyright must belong.⁵⁷⁴

The so-called *Norwich Pharmacal* order requires that three threshold conditions must be met, which place some limitations on who may submit an application: 1) a 'wrong' must have been carried out, or 'arguably carried out'; 2) the disclosure sought must be necessary to enable the applicant to bring legal proceedings or seek other legitimate redress for the wrongdoing; 3) the person against whom the order is sought must be involved in the wrongdoing in a way which distinguishes them from being a 'mere witness'. In addition, the remedy sought must be necessary and proportionate. The second of these requirements would suggest that, in copyright cases, the applicant must be the copyright holder.

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

- Please indicate whether the measures refer to public or private enforcement.

The injunction of s. 97A CDPA appears to be widely used. A number of court cases deal with such injunctions. In 2015, the IPKat suggested that over 500 websites had been blocked using this mechanism.⁵⁷⁵ An indicative list can be found on Wikipedia.⁵⁷⁶ This would be an example of a public enforcement measure.

a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?

No, the measure was inserted into the CDPA on 31 October 2003 by The Copyright and Related Rights Regulations 2003 (S.I. 2003/2498), reg. 27(1). Most of the relevant decisions appear to have been issued in 2013. The latest blocking order was issued in March 2017. It should be noted however that according to the terms of a number of the blocking orders the applicants have the right to notify

⁵⁷⁴ On this compare the wording of *Paramount v Sky* (No. 1), para. 8 with *Twentieth Century Fox Film Corporation v Sky* [2015] EWHC 1082, para. 25.

⁵⁷⁵ IPKat, '500 and Counting: Websites Blocked by Order of UK Courts', 29 July 2015, available at: <http://ipkitten.blogspot.co.uk/2015/07/500-and-counting-websites-blocked-by.html>.

⁵⁷⁶ Available at: https://en.wikipedia.org/wiki/List_of_websites_blocked_in_the_United_Kingdom.

the ISPs of new IP addresses or URLs whose sole or predominant purpose is to enable or facilitate access to the target websites.⁵⁷⁷

b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.

The following are the most high profile s. 97A CDPA cases from the last three years:

- *FAPL v BT (Football Association Premier League v British Telecommunications)* [2017] EWHC 480 (Ch)
- *Popcorn Time (Twentieth Century Fox Film Corporation v Sky UK)* [2015] EWHC 1082 (Ch) (28 April 2015).
- *1967 v Sky (1967 v British Sky Broadcasting)* [2014] EWHC 3444 (Ch) (23 October 2014);

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

There is currently a debate going on regarding who should shoulder the costs of s. 97A injunctions. This has arisen out of a trade mark case. In 2014, in *Cartier (Cartier International v British Sky Broadcasting)* [2014] EWHC 3354, the High Court found that blocking injunctions can be issued against ISPs not only for the purpose of blocking access to copyright infringing sites, but also sites that engage in trade mark infringement. The court ordered the ISPs to bear the costs of the implementation of the orders at issue. In 2016, this was confirmed by the Court of Appeal (see *Cartier International v British Sky Broadcasting* [2016] EWCA Civ 658).

There was one dissenting opinion in the CoA judgement by LJ Briggs. The judge argued that the cost of implementation of a blocking order (although not the cost of designing and installing the software with which to do so whenever ordered) should be borne by the applicant of the blocking order. LJ Briggs noted that the InfoSoc Directive and the Enforcement Directive provide respectively that the 'conditions and modalities relating to such injunctions' and the 'conditions and procedures relating to such injunctions' should be left to the national law of the Member States. He then observed that, in the case of the UK, the courts of England and Wales have jurisdiction for the grant of injunctions conferred in the most general terms, on the basis of section 37(1) of the Senior Courts Act 1981. This reflects an originally unfettered jurisdiction exercised by the Court of Chancery on equitable principles. In the case law, this has taken the form both of *Norwich Pharmacal* orders, which may require a person who has innocently become mixed up in the wrongdoing of another to provide assistance to the victim of the wrongdoing, and of Bankers Trust orders, which may require a bank to disclose the state of its customer's account, notwithstanding its duty of confidentiality to its customer, in aid of victims of a tort seeking to trace, follow or otherwise recover property of theirs which had been misappropriated by the wrongdoers. In both types of case, a standard condition or 'modality' for the grant of the injunction has historically been that the cost incurred by the innocent respondent should be reimbursed by the applicant. LJ Briggs was not persuaded that a departure from this condition is justified in cases of blocking orders for the enforcement of copyright (see para. 197-212).

The issue of costs has now been appealed to the UK Supreme Court.⁵⁷⁸ It will be interesting to see what it decides.

In addition to the above, the uncertainty at the EU level regarding the exact interpretation of the notion of a 'communication to the public' naturally also infects UK law. The important question here

⁵⁷⁷ See e.g. Annex 1 in *Twentieth Century Fox Film Corporation & Ors v Sky UK Ltd & Ors* [2015] EWHC 1082 (Ch) (28 April 2015).

⁵⁷⁸ For more information see here: <http://ipkitten.blogspot.co.uk/2017/02/the-next-round-of-cartier-uk-supreme.html>.

is whether intermediaries of various kinds can be said to be communicating works to the public and, if so, whether a mental element is necessary. Particular uncertainty surrounds modern Web 2.0 hosting platforms. The recent decision of the CJEU in *Ziggo* (C-610/15) has arguably complicated this issue.

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

I am aware of the following campaigns:

On 14 February 2014, Copyright User was launched at copyrightuser.org. This is an independent online resource produced by leading copyright academics and aimed at making UK Copyright Law accessible to creators, media professionals, entrepreneurs, students and members of the public. The site is not aimed at specific illegal/unauthorized channels. Instead, the goal is to help creators understand their rights. This objective is reflected in the FAQ, which concentrates on issues such as the term of copyright protection, authorship and ownership rules, what kind of protection is enjoyed outside of the jurisdiction, how to find copyright-free material and how to avoid infringing the work of others.

On 12 February 2015, the copyright user site incorporated two additional initiatives intended to help students and the general public understand how copyright law works:⁵⁷⁹

- ‘The Game is On!’ is an educational web series that draws inspiration from Sherlock Holmes and other well-known copyright and public domain works to provides a springboard for exploring key principles and ideas underpinning copyright law, creativity and the limits of lawful appropriation and reuse. Teachers and students can discuss these topics through the use of supplementary educational materials that accompany the video.⁵⁸⁰
- ‘Copyright for A Level Media Studies’ is an educational web resource which addresses the AS/A Level Unit ‘Critical Perspectives in Media, Section B: Contemporary Media Issues’. According to the website, the content is aimed at enabling teachers to explain the complexity and importance of copyright in media regulation and students to research copyright regulation and to demonstrate their understanding within the Contemporary Media Regulation exam question.⁵⁸¹

On 19 July 2014, an industry-led scheme called Creative Content UK was adopted by the UK’s creative industries and ISPs with the intention of promoting legal entertainment online and warning internet users whose connections are being used to illegally share films and music. The Creative Content UK initiative consists of two elements: a major multi-media public education campaign and a programme of email alerts sent by ISPs to residential broadband subscribers whose accounts are used to infringe copyright via peer-to-peer file-sharing (the VCAP system mentioned above). The resultant campaign is named ‘Get it Right from a Genuine Site’.⁵⁸² The objective is to help reduce online copyright infringement, raise awareness of the benefits that copyright brings and promote the use of legal digital content. The scheme is supported by a joint creative industry and government 3-year public education campaign towards which the government is contributing £3.5 million. The funding for this is provided jointly by the Department for Business, Innovation and Skills, the Department for Culture, Media and Sport and the Intellectual Property Office. The following organisations signed the

⁵⁷⁹ For more information, see here: www.create.ac.uk/blog/2015/02/12/what-we-should-teach-students-about-copyright.

⁵⁸⁰ For more information, see here: <http://copyrightuser.org/the-game-is-on>.

⁵⁸¹ For more information, see here: <http://copyrightuser.org/schools/a-level-media-studies>.

⁵⁸² For more information see: <https://get-it-right.org/> and <https://www.getitrightfromagenuinesite.org/>.

underlying memorandum of understanding: Motion Picture Association, British Record Music Industry (BPI), Sky, British Telecom, TalkTalk, Virgin Media.⁵⁸³

On 9 February 2017, leading UK search engine operators Google and Microsoft and entertainment trade bodies including the Motion Picture Association and music industry body BPI agreed on a Voluntary Code of Practice. This is not, strictly speaking, an education campaign, but it does aim to discourage infringement. With the Code, the search engines committed to the removal of links to websites that have been repeatedly served with copyright infringement notices from the first page of their search results. This demotion of infringing content is intended to make it much harder for UK internet users to download and stream protected content illegally. The deal was brokered by the UK Intellectual Property Office and came into force immediately. It sets targets for reducing the visibility of infringing content in search results by 1 June 2017.⁵⁸⁴

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

I am not aware of anything relevant.

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

The UK IPO has commissioned and financed a series of studies intended to track consumer attitudes and behaviours with regard to online copyright infringement and generate benchmarks and time series on the access and use of copyright material online. The latest of these (labelled as the '7th wave' study) is available here: <https://www.gov.uk/government/publications/online-copyright-infringement-tracker-survey-7th-wave>

⁵⁸³ For more information see the following links: www.creativecontentuk.org/; www.gov.uk/government/news/new-education-programme-launched-to-combat-online-piracy; www.bpi.co.uk/home/uk-creative-industries-and-isps-partner-in-major-new-initiative-to-promote-legal-online-entertainment.aspx.

⁵⁸⁴ For more information see here: <https://www.gov.uk/government/news/search-engines-and-creative-industries-sign-anti-piracy-agreement>.

Questionnaire Brazil

ALLAN ROCHA DE SOUZA, Professor of Civil and IP law at UFRRJ/ITR Law School and of Copyright and Cultural Policy at the Graduation Program on Development and Public Policy (PPED/UFRJ), Researcher at INCT Proprietas, allan@rochadesouza.com.br

and

LUCA SCHIRRU, PhD Candidate at the Graduation Program on Development and Public Policy (PPED/UFRJ). Researcher at INCT Proprietas. Lecturer in Copyright at PUC-RJ IP Course, 5211.luca@gmail.com

Last updated: 7 June 2018

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded **red**.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.

Taking from the broader legal system, we may identify the following as having direct and indirect application:

- Brazilian Federal Constitution (Constituição da República Federativa do Brasil de 1988: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm;) In English: http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/Constitution_2013.pdf . Articles 5º, XXVII, XXVIII e XIX.
- Copyright Act (Lei nº 9.610/98 - Lei de Direitos Autorais: http://www.planalto.gov.br/ccivil_03/leis/L9610.htm). English version: http://www.wipo.int/wipolex/en/text.jsp?file_id=125393. Arts. 101-110; art.29.
- Software Protection Act (Lei nº 9.609/98 - Lei de Software: http://www.planalto.gov.br/ccivil_03/leis/L9609.htm). English version: http://www.wipo.int/wipolex/en/text.jsp?file_id=125391. Arts. 12, 13 e 14.
- Penal Code (Decreto Lei nº 2.848/1940 - Código Penal: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm). Arts. 184 e 186.

- Civil Code (Lei nº 10.406/2002 Código Civil: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm). Arts. 186-187, 927-943.
- Consumer Rights Code (Lei no 8078/90 Código de Defesa do Consumidor: http://www.planalto.gov.br/ccivil_03/leis/L8078.htm).
- Internet Civil Act (Lei nº 12.965/2014 - Marco Civil da Internet: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm). English Version: <https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180> Arts. 19§2º, 31.

The most important legislation is the Copyright Act. However, the extent of its commands cannot be fully understood if one does not bring into account the other (potentially) applicable norms, not only because the Copyright Act lacks serious update (it was updated in respect to collective management in 2013, but otherwise remains the same as when came into effect, in June 1998), but also due to its incompleteness and sometimes contradictory nature.

That said, one must first look into the Constitution for guidance on the balancing of rights and interests and individual fundamental rights and guarantees. Copyright criminal offenses are provided for in the Penal Code. Contractual infringement and damage responsibilities are mainly spread throughout the Civil Code. The Software Protection Act is expressly complemented by the Copyright Act.

The Internet Civil Act in spite of establishing “principles, guarantees, rights and obligations for the use of the internet in Brazil”, expressly excludes Copyright from its provisions, as per arts. 19 and 31:

Art. 19. In order to ensure freedom of expression and prevent censorship, the provider of internet applications can only be subject to civil liability for damages resulting from content generated by third parties if, after a specific court order, it does not take any steps to, within the framework of their service and within the time stated in the order, make unavailable the content that was identified as being unlawful, unless otherwise provided by law. (...)

§ 2o The implementation of the provisions of this article for infringement of copyright or related rights is subject to a specific legal provision, which must respect freedom of speech and other guarantees provided for in art. 5o of the Federal Constitution.

Art. 31. Until the entry into force of specific law provided for in § 2o of art. 19, the liability of the internet applications provider for damages arising from content generated by third parties, in case of copyright or related rights infringement, shall continue to be governed by applicable copyright legislation in force, at the time of entry into force of this Law.

As of May 2018, the House of Representatives is discussing a Law project regulating Personal Data. It mirrors substantially the recent EU General Data Protection Regulation.⁵⁸⁵ It is expected that, at least indirectly, it will impact some of the measures in respect to copyright infringement.

So, for lack of specific regulation of digital infringement and ISP responsibilities/safe harbours, the solution lies on the interplay between the different applicable norms.

2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?

⁵⁸⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

The Internet Civil Act provides the following definitions for different intermediaries:

Art. 5^o For the purposes of this Law, the following concepts apply:

I - internet: the system consisting of the set of logical protocols, structured on a global scale for public and unrestricted use, in order to enable communication of data between terminals, through different networks;

II - terminal: a computer or any device that connects to the internet;

III - internet protocol address (IP address): the code assigned to a terminal from a network to enable their identification, defined according to international standards;

IV - autonomous system administrator: an individual or legal entity that administrate specific blocks of IP addresses and its specific autonomous routing system, duly registered in the national entity responsible for the geographically registration and distribution of IP addresses related to the Country;

V - internet connection: the enabling of a terminal for sending and receiving data packets over the Internet, by assigning or by authenticating an IP address;

VI - connection record/log: the set of information pertaining to the date and time of the beginning and end of a connection to the internet, the duration thereof and the IP address used by the terminal to send and receive data packages;

VII - Internet applications: a set of functionalities that can be accessed through a terminal connected to the Internet; and

VIII - registrations of access to Internet applications: the set of information regarding the date and time of use of a particular internet application from a particular IP address.

In spite of the fact that this legislation treats extensively on the different types of providers it does not give any definition on them.

3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
- Depends on the commercial or for-profit nature or intent of the use or user;
- Is uncertain and, if so, why;
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

There are no dispositions specifically qualifying the copyright digital infringement acts. The reason for this is that the Copyright Act is from 1998, and it has only been updated regarding Collective Management.

It is important to notice that the Penal Code provisions could be potentially applicable to different cases, as well as the Civil Code.

The general provisions potentially (for the need of conceptual adaptation) applicable to digital infringement within the Copyright Act are the following:

Title VII Sanctions for copyright Infringement

Chapter I Introductory Provision

101. *The civil sanctions provided for in the following Chapter shall be applicable without prejudice to criminal sanctions.*

Chapter II Civil Sanctions

102. *Any owner of rights whose work is fraudulently reproduced, disclosed or used in any other way may apply for the seizure of the copies or originals made or the stoppage of the disclosure, without prejudice to whatever indemnification may be applicable.*

103. *Any person who publishes a literary, artistic or scientific work without the authorization of the owner of the copyright shall forfeit to the latter the copies that are seized and shall pay him the price of those that have been sold. Sole paragraph. Where the number of copies constituting the fraudulent edition is unknown, the offender shall pay the value of 3,000 copies in addition to the copies seized.*

104. *Any person who, for the purposes of sale or the securing of direct or indirect gains, advantages or profits for himself or for another, sells, displays for sale, receives and conceals, acquires, distributes, keeps on deposit or uses a fraudulently reproduced work or phonogram shall be jointly liable with the infringer in terms of the foregoing Articles; if the reproduction has been carried out abroad, the importer and the distributor shall answer for the infringement.*

105. *The transmission and retransmission by any means or process and the communication to the public of literary, artistic and scientific works, performances and phonograms carried out in violation of the rights of the owners shall be immediately discontinued or interrupted by the competent judicial authority, without prejudice to a daily coercive fine for non-observance and such other indemnities as may be applicable, and without regard to the applicable criminal sanctions. Where the offender is found guilty of recidivism in the infringement of the rights of owners of authors' rights or neighboring rights, the amount of the fine may be doubled.*

107. *Without regard to the seizure of the equipment used, any person shall be liable to damages in an amount not less than that resulting from application of the provisions of Article 103 and its sole paragraph who:*

I. *alters, removes, modifies or in any way disables technical devices that have been incorporated in copies of protected works and productions to prevent or restrict reproduction;*

II. *alters, removes or in any way spoils the encrypted signals intended to restrict the communication to the public of protected works, productions or broadcasts or to prevent the copying thereof;*

III. *without authorization removes or alters any rights management information;*

IV. *without authorization distributes, imports for distribution, broadcasts, communicates or makes available to the public works, performances, copies of performances fixed on phonograms and broadcasts in the knowledge that the rights management information, the encrypted signals and the technical devices have been removed or altered without authorization.*

Considering the fact that the legislation is unfit for dealing properly with the digital scenario, one must always take into account the general provisions providing for economic exclusive rights for right-holders on articles 29 and 30 below, where the key terms are highlighted:

29. *The express prior authorization of the author of a literary, artistic or scientific work shall be required for any kind of use, such as*

I. *complete or partial reproduction;*

II. *publication;*

III. *adaptation, setting to music or any other transformation;*

IV. *translation into any language;*

V. *incorporation in a phonogram or in an audiovisual production;*

VI. *distribution where it is not provided for in a contract signed by the author with third parties for the use or exploitation of the work;*

VII. distribution *for the purposes of offering works or productions by cable, optic fiber, satellite, electromagnetic waves or any other system enabling the user to select a work or production and receive it at the time and place of his choice, provided that the access to the works or productions is made through any system requiring payment on the part of the user;*

VIII. *the direct or indirect use of the literary, artistic or scientific work in one of the following forms:*

- (a) performance, recitation or declamation;*
- (b) musical performance;*
- (c) use of loudspeaker or comparable systems;*
- (d) radio or television broadcasting;*
- (e) reception of a radio broadcast in places frequented by the public;*
- (f) provision of background music;*
- (g) audiovisual, cinematographic or equivalent presentation;*
- (h) use of man-made satellites;*
- (i) use of optical systems, telephone or other lines, cables of all kinds and such comparable means of communication as may be devised in the future;*
- (j) exhibition of works of three-dimensional and figurative art;*

IX. *incorporation in databases, storage in a computer, microfilming and any other means of archiving of that kind;*

X. any other form *of use that exists at present or might be devised in the future.*

30. *In the exercise of the right of reproduction, the owner of copyright may make the work available to the public in whatever form and place and for whatever time that he considers appropriate, either for a consideration or free of charge.*

(1) *The exclusive right of reproduction shall not be applicable where the reproduction is temporary and done for the sole purposes of making the work, phonogram or performance perceptible by means of an electronic medium, or where it is transitory or incidental, provided that it is done in the course of the use of the work that has been duly authorized by the owner.*

(2) *Regardless of the manner of reproduction, the number of copies made shall be notified and checked, the person who reproduces the work being responsible for the keeping of such registers as will permit the author to verify the economic profits derived from exploitation.*

When analyzing the questions below, one must consider that most of the applicable restrictions on uses by third parties or the consideration of infringement will fall into the general and broad category of “use/utilization rights”, which is to include all sorts of possible uses not otherwise specified.

a) Downloading copyright-protected content from illegal/unauthorized sources on the Internet.

There are no dispositions specifically qualifying such copyright digital infringement act. Please see answer to question 3, above.

For the individual end user, in the unlikely possibility he is made responsible for downloading, it would come as “reproduction rights” or the more general “use rights” (a broad term encompassing all sorts of uses that made its way into the legislation). The Penal Code expressly excludes individual private copy from criminal responsibility. Whereas for civil liability the “short excerpts” and the “family and intimate private use” exceptions could exempt acts of downloading..

The most possible violation, if any, although unlikely to be considered as such, would be against reproduction rights (or the general “use rights” mentioned above), for the reproduction of entire works without permission (see generally art. 102 of the Copyright Act). However, I am unaware of any specific case brought to the higher Courts.

b) Streaming copyright-protected content from illegal/unauthorized sources on the Internet.

There are no dispositions specifically qualifying such copyright digital infringement act.

It would violate the distribution rights of right-holders as well as broadcasters' signal rights. Transmission and retransmission rights could also be violated. Please refer to article 105 of the Copyright Act (mentioned in the preliminary remarks to Question 3 above). However, I am unaware of any specific case brought to the higher Courts arguing for copyright violation.

Considering the act of receiving streaming from illegal sources, we must first disregard the application of the exception for temporary/transient reproduction, since it must occur in the course of an authorized use, which is not the case. However, regardless of the exception, there is no disposition directed to the end-users themselves. Depending on how the whole process is done, it could possibly violate the Communications Act or be considered a signal theft, but it is, in my opinion, very uncertain and extremely unlikely. (See also above our answer to Question 3-a).

c) Stream-ripping copyright-protected content.

There are no dispositions specifically qualifying such copyright digital infringement act. Please see preliminary remarks to Question 3 above. The most likely violation would be against reproduction rights, for the reproduction of entire works without permission (art. 102 of the Copyright Act). However, I am unaware of any specific case brought to the higher Courts.

One could refer to the general download comments (3.a) for further grasping of the situation.

If the stream-ripping does include altering or disabling any TPM, then we would have a violation of art. 107 of the Copyright Act, subject to civil responsibility.

d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.

There are no dispositions specifically qualifying such copyright digital infringement act. Please see preliminary remarks to Question 3 above, especially articles 104 and 105 of the Copyright Act. It would likely violate the communication to the public, "making available", and distribution rights.

e) Posting hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.

- Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard surface hyperlink, deep-link, embedded or framing hyperlink).

Legal Scholarship generally agrees that there is no violation in inserting a hyperlink to copyrighted material. However, if the link is to an illegitimate or violating source, and one profits from the hyperlink, one could be potentially considered solidary in perpetrating the violation and subject to the joint liability compensation for damages. In any case, there are no dispositions specifically qualifying such copyright digital infringement act. Please see preliminary remarks to Question 3 above, especially article 104 of the Copyright Act.

f) The sale of Kodiboxes or similar devices.

There are no dispositions specifically qualifying such copyright digital infringement act. In fact, they are, to our knowledge, not so popular in Brazil – although similar devices are advertised and may become more used and popular.

However, in our opinion, the sales of Kodiboxes with included unauthorized add-ons would qualify as violation, whether that is of communication, distribution or transmission rights or fall in the general category of "use/utility" rights ("direito de utilização"). By stretching its meaning, we could apply the

articles 104 or 105 to the sellers/distributors. As per the buyers and user we should refer to question 3.a regarding downloading.

g) Other types of unauthorized online use of copyright-protected content not listed above.

As mentioned above, the Copyright Act has not been updated to face the digital challenges, except for collective management. So, for all types of digital violation, one shall look to article 29 and 30 of the Copyright Act for the establishment of the author and right-holders' rights and entitlements. Therefore, it remains a strong exercise of analogy to fit supposed digital violations into the analogical framework.

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

Not specifically when related to Copyright. As a general rule, 18 years old and above are criminally responsible for their acts. There are different degrees of sanctions for those younger than 16, depending whether they are in the 16-18 years old range, between 12 and 15 or below 12 years old.

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country's law? If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.

The Internet Civil Act provides liability exemptions for intermediaries. However, as mentioned above, Copyright was specifically excluded from its scope. In any case, the legal dispositions are the following (art. 18, 19§2º, 21):

Art. 18. The provider of connection to internet shall not be liable for civil damages resulting from content generated by third parties.

Art. 19. In order to ensure freedom of expression and prevent censorship, the provider of internet applications can only be subject to civil liability for damages resulting from content generated by third parties if, after an specific court order, it does not take any steps to, within the framework of their service and within the time stated in the order, make unavailable the content that was identified as being unlawful, unless otherwise provided by law.

(...)

§ 2º The implementation of the provisions of this article for infringement of copyright or related rights is subject to a specific legal provision, which must respect freedom of speech and other guarantees provided for in art. 5º of the Federal Constitution.

Art. 21. The internet application provider that makes third party generated content available shall be held liable for the breach of privacy arising from the disclosure of images, videos and other materials containing nudity or sexual activities of a private nature, without the authorization of the participants, when, after receipt of notice by the participant or his/hers legal representative, refrains from removing, in a diligent manner, within its own technical limitations, such content.

Sole Paragraph. The notice set forth above must contain sufficient elements that allow the specific identification of the material said to violate the right to privacy of the participant-user and the confirmation of the legitimacy of the party presenting the request.

It is of special importance to this report the recent case brought to the Supreme Court (Recurso Extraordinário n. 1.037.396/SP), which has been accepted for review by the Court and qualified as of "broad interest/repercussão geral". The case is about a decision by the São Paulo State Court that decided for the strict liability of an ISP, and considered Article 19 of the Internet Civil Act unconstitutional on the grounds that it requires a Court order also in relation to content that violates honor and intimacy; according to this court, the ISP must in these cases act upon a simple notice to make unavailable the unlawful content. At time of writing, no date has been set for the Supreme Court to decide on this case.

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

There is uncertainty on how the ISP would be liable. Although unlikely to be primarily responsible for the infringement, it is subject to secondary and/or subsidiary liability.

As mentioned above, they do not benefit from safe harbours established by the Internet Civil Act regarding copyright infringement, as it refers (art. 19, 2) to the need for an updated legislation and, in the meanwhile, the legislation in place, which is the 1998 Copyright Act.

The 1998 Copyright Act, on article 104, determines that contributors to copyright and related rights' infringement should be jointly liable, and, on article 105, that the infringement shall be interrupted by the judicial authority (that is, as a result of a legal decision like an injunction and not a simple notice).

No legislation has yet satisfactorily faced the problem. So, Courts – since before the Internet Civil Act – have found support for making the ISP responsible by referring to the general civil responsibility in the Civil Code as well as the Consumer Rights Code, as detailed further down at Question 8A.

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:

- The suspension from the Internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.
- The monitoring or **filtering** of content.
- The **blocking** and removing of infringing content, including notice-and-takedown.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- **Graduated response systems.**

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- *When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).*

As a preliminary remark, there are no significant differences to report depending on the type of protected content.

b) Civil.

The Copyright Act establishes civil penalties for copyright infringement – both injunctions and damages - in its arts. 102 to 110. The most relevant provisions are set forth below (the remaining articles can be consulted at http://www.wipo.int/wipolex/en/text.jsp?file_id=125393):

102. Any owner of rights whose work is fraudulently reproduced, disclosed or used in any other way may apply for the seizure of the copies or originals made or the stoppage of the disclosure, without prejudice to whatever indemnification may be applicable.

103. Any person who publishes a literary, artistic or scientific work without the authorization of the owner of the copyright shall forfeit to the latter the copies that are seized and shall pay him the price of those that have been sold.

Sole paragraph. *Where the number of copies constituting the fraudulent edition is unknown, the offender shall pay the value of 3,000 copies in addition to the copies seized.*

105. The transmission and retransmission by any means or process and the communication to the public of literary, artistic and scientific works, performances and phonograms carried out in violation of the rights of the owners shall be immediately discontinued or interrupted by the competent judicial authority, without prejudice to a daily coercive fine for non-observance and such other indemnities as may be applicable, and without regard to the applicable criminal sanctions. Where the offender is found guilty of recidivism in the infringement of the rights of owners of authors' rights or neighboring rights, the amount of the fine may be doubled.

106. The sentence may include the obligation to destroy all unlawful copies and originals, and also the blocks, molds, negatives and other material used to commit the infringement; and it may provide for the seizure of machines, equipment and materials used for the purpose, including their destruction where they can only serve unlawful purposes.

As noted above (see preliminary remarks to Question 3), Brazilian copyright law has not been adjusted to the specificities of online use. The same is true for enforcement measures. That means that existing law applies to online use by analogy. For example:

- In applying article 103, sole paragraph, one would refer to the total number of reproductions but would have to adjust the damages to a proportionate amount (if they are disproportionately large).
- Article 105 could be the basis of an injunction and coercive fine for individuals and online platforms making available works without the authorization of rights holders, such as The Pirate Bay;
- Article 106 could be used to order the destructions of equipment used to host unauthorized copies of works (such as computers).

The Courts have very recently held the understanding that, once notified, the ISP becomes co-responsible of copyright infringement if it does not take the work down (Please see answer to Question 8A for a description of the relevant case law). Such decision reinforces the system of notice and take down, put independently in place by right-holders and ISP. However, I would not say it is definite yet.

c) Administrative.

Not available.

d) Criminal.

Copyright infringement is a crime typified in the Brazilian Penal Code and its regulation varies according to certain characteristics of the violation, as follows:

Infringement	Penalty	Pecuniary Fine	Legal Measures
Art. 184: To infringe copyright and related rights	Detention: from three months to one year or fine	Possible as an alternative to detention.	Depends on a Crime Complaint by the rights holder.
Art. 184, § 1: If the infringement consists of a total or partial reproduction for the purpose of direct or indirect profit, by any means or process, of copyrighted works, interpretation, performance or phonogram, without the express authorization of the author, the performer or the producer. Or if, for the purpose of direct or indirect profit, it distributes, sells, exhibits for sale, leases, introduces in the country, acquires, hides, holds in storage, original or copy of intellectual work or phonogram reproduced by infringement of copyright, performer rights, phonogram rights, or, alternatively, rents original or copy of an intellectual work or phonogram, without the express authorization of the rightholders or of those who represent them	Detention: from two to four years and fine	Yes, in addition to detention.	Independent of Criminal Complaint from right holder. It is public criminal action.
Art. 184, § 2o. Incurs in the same penalty of § 1o, anyone who, for the purpose of direct or indirect profit, distributes, sells, exhibits for sale, rents, introduces in the Country, acquires, hides, has in store, original or copy of intellectual work or phonogram reproduced with infringement of copyright, the right of the performer or the right of the phonogram producer, or, alternatively, rents original or copy of an intellectual work or phonogram, without the express authorization of the rightholders or their representative.	Detention: from two to four years and fine	Yes, in addition to detention.	Independent of Criminal Complaint from right holder. It is public criminal action.
Art. 184, § 3. If Violation of copyright that consists of offering to the public, by cable, fiber optic, satellite, waves or any other system that allows the user to perform the selection of the work or production to receive it at a time and place previously determined by those who formulate the demand, for the purpose of profit, direct or indirect, without express authorization, as the case may be, of the author, the performer, the phonogram producer, or who represents them	Detention, from two to four years	Yes, in addition to detention.	Public criminal action dependent on representation by right holder

Infringement	Penalty	Pecuniary Fine	Legal Measures
Art. 184, § 4o. Paragraphs 1, 2 and 3 do not apply in the case of an exception or limitation to copyright or those related thereto, in accordance with the provisions of Law No. 9.610 of February 19, 1998, nor the single copy of an intellectual work or phonogram for the private use of the copyist, with no direct or indirect profit.	No Penalty is applicable	No fine is applicable	Exempt from criminal penalty

Pursuant to Art. 184, § 4 of the Penal Code, none of the above crimes applies that if the act in question is covered by an exception or limitation, or if the copier makes one single copy of the work/subject matter for private use and without the purpose of direct or indirect profit. This would mean that acts of downloading (Question 3.a above) and stream ripping (Question 3.c above) do not give rise to criminal liability. On the other hand, acts of uploading and active streaming to the public would give rise to liability under Art. 184, § 3 of the Penal Code. All other acts of infringement would possibly fall under the general clause of Art. 184.

Furthermore, in crimes committed against public entities, autarchies, public companies, mixed-economy societies or foundations established by the Public Authorities, the legal measures to be adopted would be the unconditional public criminal action, meaning no representation by the rightsholder is needed.

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law against intermediaries to address online copyright infringement by third party users of their services?

- *When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).*

As a preliminary remark, there are no differences to report depending on the type of protected content. That said, the responsibility of intermediaries will depend on a few elements that will be described in the answers to the following questions.

a) Civil.

Regarding the responsibility of the providers, we refer to Question 5 above, where we discuss the responsibility of the intermediaries under the Internet Civil Act. It is important to emphasize that such rules do not cover copyright, and the status quo is maintained accordingly.

Four cases are key to understanding the liability of intermediaries for copyright violations from the perspective of the Superior Court of Justice – STJ as of now. The STJ was selected based on its constitutional competence for harmonizing the interpretation of federal legislation. At the same time, the selected leading cases have faced the key question and established likely precedents for lower courts and future understandings.

The cases are the following: Special (i) Appeals (Recurso Especial) nº 1.512.647/15; (ii) nº 1.396.417/13; (iii) nº 1.328.706/13; and (iv) a group of decisions at different levels on the same case:

Agravo no Recurso Especial (AREsp) nº 259.482/13⁵⁸⁶; Agravo Regimental no Agravo no Recurso Especial (AgRg no AREsp) nº 259.482/13⁵⁸⁷.

It is noteworthy to highlight that the Copyright Act was not used to establish the liability, even though it refers to copyright violation and to decide on the ISP liability for copyright infringement. In the absence of a specific legislation regulating it, the courts have resorted to both the Consumer Rights Code and the Civil Code general civil responsibility norms. Also important is the fact that the cases refer to situations prior to the entering into force of the Internet Civil Act, but seem to have clearly influenced the results and compromises then reached.

Starting with the decisions (AREsp 259.482/13 and Ag no AREsp 259.482/13) denying review of the state court of appeals decision (Tribunal de Justiça de Minas Gerais) around Google's responsibility for copyright violation by a user who made educational material available online in a blog. The State Court decision deemed Google, as the host provider, responsible for the violation, and condemned it on moral damages, because it did not take the content down immediately after being notified by the victim, doing so only after a Court order. What we see as important here is the fact that the secondary liability/subsidiary responsibility of the ISP depends on a private notice of the violation, and not from the Court order. In the rationale, the decisions say it is applicable both the Civil Code and Consumer Rights Code to the case, but state that the ISP cannot be deemed objectively responsible for the violation or assume the risks of the violation unless it does not act once informed of the violation.

In the Special Appeal nº 1.328.706/13, where damages are sought after educational material was uploaded on a blog, it is decided that Google, as the host provider, is not obliged to review postings by users, but however, once informed of the violation, it must act to take down the infringing content within 24hs, or be deemed co-responsible for the infringement. Two key aspects are of special importance. First, it must take the content down immediately but temporarily, since it must find ways to decide whether the act is really a violation or not, and if it decides it is not a violation, must put it back up. The Court recognizes that Google does have a system of securing against violations in its terms and conditions. Secondly, the alleged victim must specify the offensive content to be taken down as well as provide the exact URL in order to allow for the taking down without offending collective rights to information and freedom of expression, for example.

The Special Appeal nº 1.396.417/13 reinforces what has been said in the case above mentioned.

As for the Special Appeal nº 1.512.647/15, a few different nuances are added to the building understanding of ISP liability: (i) one refers to the fact that the use in question does not fall within the limitations (the rapporteur expressly refers to 'fair-use'); (ii) the primary function of the network or internet application (ORKUT) is not file sharing but, in the case, personal relationship and social networking; (iii) there aren't, in the case, damages to the plaintiff that can be imposed on the ISP for failing to act to stop the violation; (iv) there is no evidence of Google profiting from the third party copyright violation. Such criteria are added to those established in the prior decisions mentioned (plaintiff informing the exact URL and description of the violation plus ISP duty to take down the content upon notice), in order to determine the contemporary contours of ISP liability in Brazil for Copyright violations.

On top of that, the last decision also reinstates that the ISP liability issues don't fit easily within the scope of the 1998 Copyright Act (art. 102 to 104) and that it is applicable in such cases the general tort rules at the Civil Code and Consumer Rights Code. Interesting to note that here we have the same plaintiff and defender as in the Special Appeal nº 1.328.706/13, but referring to a different violation, although in the same circumstances.

⁵⁸⁶https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=MON&sequencial=27549935&num_registro=201202452491&data=20130319

⁵⁸⁷https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1225897&num_registro=201202452491&data=20130430&formato=PDF

It is also interesting to notice the very recent Santa Catarina (State) Court Decisions on a related case (AC 0000412-86.2016.8.24.0175, and AC n. 0000447-46.2016.8.24.0175), whereby Google was condemned for not having restored the content up on YouTube after the counter-notice by the user assuring it was a parody protected by a limitation to copyright, as it should have done.

b) Administrative.

Not applicable.

c) Criminal.

Not applicable.

9. To the best of your knowledge, are there significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

Regarding the kind of content there is no difference.

However, there is an incongruity between public norms, court decisions and private practice. That is so because the 1998 Copyright Act points to the need for a judicial decision to oblige ISP to withdraw content from the internet, the Internet Civil Act excludes copyright from safe harbors and the Civil and Consumer Rights Codes establish only general guidance on the matter. We must also notice that ISP may withdraw content if it decides it breaks its terms and conditions, that is, by contractual rules.

Article 102 says the right-holder “may apply to”, meaning it needs a decision - a Court order – or even Administrative, if there was one - to act on seizing the copies or equipment or stopping the infringing acts.

At the same time, the STJ has ruled that the non-compliance with an out-of-court notification (notice and take down) is enough to prove a copyright infringement by an intermediary subject to reparation (see answer to Question 8A)

When Courts accept the ISP Joint Liability when not acting on the right holders’ notification of infringement, they are accepting that such a simple notification as sufficient.

It is also important to note that some criminal types related to copyright infringement demand initiative on the part of the injured party, as in the case of private criminal action where criminal proceedings are to be conducted through a criminal complaint or representation.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

According to the Internet Civil Act, there are no obligations of such nature regarding copyright infringement. Despite this, the Internet Civil Act deals with the custody of records and personal data, including the availability of personal data, as follows in its art. 10, transcribed below.

***Art. 10.** The retention and the making available of connection logs and access to internet applications logs to which this law refers to, as well as, of personal data and of the content of private communications, must comply with the protection of privacy, of the private life, of the honor and of the image of the parties that are directly or indirectly involved.*

§ 1o – The provider responsible for the retention of the records as set for in art. 10o shall only be obliged to provide them, whether separately or associated with personal data or other information that allows the identification of the user or of the terminal, upon a judicial order, as provided in Section IV of this Chapter, in compliance with what is set forth in art. 7o.

§ 2o – The content of private communications may only be made available by court order, in the cases and in the manner established by law, and in compliance with items II and III of art. 7o.

§ 3o – The provision of the caput of art. 10 does not prevent administrative authorities to have access to recorded data that informs personal qualification, affiliation and address, as provided by law.

§ 4o – The security and confidentiality measures and procedures shall be informed in a clear manner by the responsible for the provision of the services, and meet the standards set in regulation, in compliance with rights of confidentiality of business secrets.

Although the Internet Civil Act does not apply to copyright, copyright owners may nonetheless request and obtain personal data in infringement proceedings. To do so, they can file a claim for copyright infringement (under arts. 102 and 104 of the Copyright Act) and thereafter refer to the general obligation in art. 10 of the Internet Civil Act according to which ISPs must retain personal data. Since ISPs must comply with this obligation, it is feasible for copyright owners to obtain personal data of infringers in this way through a Court order. That is to say, if they establish the necessary requirements for an infringement claim under the Copyright Act, they may request the Court to order ISPs to provide them with the necessary information to pursue that infringement, which information they have in their possession as a result of the general obligation under art. 10 of the Internet Civil Act. As for before the Internet Civil Act, one could base the request on the general responsibility rules established by the Civil Code and Consumer Rights Code – as explained on the answer to Question 8A.

a) If yes, what conditions must be met for that obligation to arise?

As mentioned above, even though the Internet Civil Act excludes ISP liability regarding copyright infringement by third parties from its norm-setting (art. 19, 1o and 2o), it does not exclude ISP from other obligations, such as those established on article 10.

So, the data must be provided in a justified manner and in accordance to the Court Order, and the confidentiality of the information received is guaranteed to preserve the intimacy, privacy, honor and image of the user, including, to consider the case as a “secret of justice”. See below the relevant provisions in the Internet Civil Act:

Art. 22. The interested party may, for the purpose of providing evidence in civil or criminal legal procedures, in character incidental or autonomous, require the Judge to order the entity responsible for the keeping of records to provide the connection or access logs to internet applications.

Sole Paragraph. Without prejudice of other legal requirements, the request shall contain, under penalty of inadmissibility:

I - justified evidence of the occurrence of the illicit act;

II - motivated justification of the usefulness of the requested records for investigation or probative instruction; and

III - the period of time to which the records correspond.

Art. 23. It is the duty of the Judge to take the necessary measures to ensure confidentiality of received information and the preservation of intimacy, privacy, honor and image of the user. The Judge may determine “secrecy of justice” on the case, including with respect to the requests for record retention.

In the decree that regulates the Internet Civil Act (**Decree No. 8.771/2016**) there are provisions on the matter of the storage, custody and processing of personal data, which are of great importance for the present study, despite the exclusion of copyright from the scope of this Act, as shown above:

***Article 13.** Connection and application providers shall, in the custody, storage and processing of personal data and private communications, observe the following safety standards guidelines:*

***I** - the establishment of strict control over access to data by defining the responsibilities of persons who will have access possibilities and privileges of exclusive access for certain users; (...)*

***Paragraph 2** - In view of the provisions in items VII to X of the caput of art. 7 of Law No. 12,965, of 2014, connection and application providers must retain the smallest possible amount of personal data, private communications, and applications access and connection records, which should be excluded:*

***I** - as soon as the purpose of its use is reached; or*

***II** - if the term determined by legal obligation is expired.*

b) If yes, what type of personal data is typically requested?

The law does not establish what data should be transmitted, but indicates that such data should contribute to the identification of the user or terminal which access is wanted. However, the Decree regulating Internet Civil Act (Decree No. 8.771/2016, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm) provides for registration data:

***Art. 11.** The administrative authorities referred to in art. 10, paragraph 3 of Law No. 12,965, of 2014 shall indicate the legal basis of express jurisdiction for access and motivation for the request for access to the registration data.*

***Paragraph 1.** The provider that does not collect registration data shall inform the requesting authority of this fact and shall not be required to provide such data.*

***Paragraph 2.** The following are considered as registration data:*

***I** - affiliation;*

***II** - the address; and*

***III** - personal qualification, understood as name, first name, marital status and profession of the user.*

***Paragraph 3** - The requests referred to in the caput must specify the individuals whose data are being requested and the information desired, being generic or non-specific collective requests forbidden.*

Still, in its art. 14, this decree establishes what is personal data:

***Art. 14.** For the purposes of the provisions of this Decree, it is considered:*

***I** - **personal data** - data related to the identified or identifiable natural person, including identification numbers, locational data or electronic identifiers, when these are related to a person; and*

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

In the civil sphere, copyright holders must act themselves, as defined in the Copyright Act. Also, within the limits of the respective assignment or license of rights, the assignee or licensee may apply for enforcement measures. Collective Management Organizations could do so as well, as long as the infringement falls within their representation powers.

With regards to the criminal sphere, it will depend on the type of criminal offense: that may be the right holder in cases of private criminal action or public criminal action conditioned to representation,

or the Public Prosecutor's Office in the crimes that will be tried in unconditional public criminal action, according to the Brazilian Criminal Procedure Code.

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

- Please indicate whether the measures refer to public or private enforcement.

The actions that have shown greater effectiveness are those carried out directly against the intermediaries, especially those of private character, such as the sending of out-of-court notifications and the notice-and-takedown system.

a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?

The sending of out-of-court notifications and the notice-and-takedown system was not expressly established by law in Brazil. Courts have established the subsidiary liability under certain conditions – most importantly be notified by the victim –, which has now become relevant because of private practice.

b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.

The cases have been presented at Question 8A. Be aware that though

- STJ Recurso Especial Nº 1.512.647, from May 13, 2015 (<https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1395049&tipo=0&nreg=201301628832&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20150805&formato=PDF&salvar=false>). This is the leading case on the matter of ISP liability for copyright infringement so far. It establishes secondary liability of ISP if one doesn't make the URL of the infringing material (to be unequivocally informed by the plaintiff through notice) inaccessible after being notified by the interested party. It also establishes that the primary function of the application, software or platform in question must not be to promote infringement primarily for infringement (e.g. as would be the case for Pirate bay), or that would lead to a finding of contributory responsibility.
- On the same line, both in 2013 at STJ (Recurso Especial Nº 1.396.417⁵⁸⁸, from November 07, and Recurso Especial Nº 1.328.706⁵⁸⁹, from October 15). It establishes, in short, that ISP are subject to the Consumer Rights Code and are therefore objectively responsible for damages caused to others for risks inherent to the activity, but that ISP are not to be deemed responsible in the case of copyright violation (because of freedom of expression rights) if it does temporarily remove the content within 24h of being notified, until further verification by the ISP.
- STJ Agravo no Recurso Especial 259.482.. In this case, Google was ordered to pay material and moral damages to the author of the material that was made available in her blog. Google

⁵⁸⁸

https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1279538&num_registro=201302517510&data=20131125&formato=PDF

⁵⁸⁹

https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1273201&num_registro=201201225460&data=20131213&formato=PDF

was convicted and liable for material and moral damages "for failing to withdraw immediately after the knowing of the illegality of the posted material, which bore the name of its creator."

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

We can highlight three points of importance in the debates about copyright infringement on the Internet: the mechanisms of content withdrawal from the Internet, notably the Notice-and-Notice and Notice-and-Takedown; the liability of ISPs as to the illegal content; the preservation of limitations and exceptions in the digital environment and how they interact with private contractual conditions; and the amount of compensation due.

- By Notice and Notice we mean the system by which either one's content is not taken down before the possibility of responding by accepting the notification or assuming the risk of the violation and keeping it up or it is taken down temporarily until one's response to put it back up.
- The liability of providers has been explained all through the document and more specifically on answer to question 8A.
- The amount of compensation due for infringement is set in the general tort rules that calls for proportionality of when establishing the amount due for damages, especially in the case of presumed damages.

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

Several campaigns were done in an online environment and in the media, among which we highlight the following:

- Campaign Name: Piracy is not cool! (Pirataria não é legal!)

Most Focused Media / Products: Piracy in General.

Agents involved in the campaign: conducted by the Brazilian Licensing Association – (Associação Brasileira de Licenciamento – ABRAL), with the support of the National Council for Combating Piracy and Crimes against Intellectual Property (Conselho Nacional de Combate à Pirataria e Delitos Contra a Propriedade Intelectual – CNCP); the National Forum Against Piracy and Illegality (Fórum Nacional Contra a Pirataria e Ilegalidade – FNCP) and the Institute of Intellectual Capital (Instituto do Capital Intelectual – ICI);

Media used: Ads and vignettes were made available for free to all media and materials were transmitted on Cultural and Cartoon Networks.

- Campaign Name: Report Piracy. (Denuncie Pirataria)

Most Focused Media / Products: Software.

Agents Involved in the Campaign: Created by ABES and BSA - The Software Alliance;

Media used: internet.

- Campaign Name: Piracy: I'm Out! Long live Originality. (Pirataria: Tô Fora! Viva a Originalidade)

Most Focused Media / Products: Piracy in General.

Agents involved in the campaign: promoted by the National Union of Tax-Analysts of the Brazilian IRS - Sindireceita, with the support of the National Council to Combat Piracy of the Ministry of Justice (Conselho Nacional de Combate à Pirataria do Ministério da Justiça - CNCP / MJ).

Media used: events and the internet, mainly.

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

Nothing to report.

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

To our knowledge, there aren't any reliable published studies of the kind.

Questionnaire Canada

DAVID FEWER, Executive Director Samuel-Glushko – CIPPIC (Centre for Law, Technology and Society), University of Ottawa

Last updated: 12 June 2018

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded **red**.

Legal Rules on Online Copyright Infringement

- 1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.**

Copyright Act (R.S.C., 1985, c. C-42).⁵⁹⁰ Hereafter the “*Copyright Act*”.

- 2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?**

2.4(1)(b)⁵⁹¹ to the *Copyright Act* which provides that persons who only supply “the means of telecommunication necessary for another person to so communicate” are not themselves to be considered parties to an infringing communication.

User generated content:

In the context of provisions concerning user generated content the *Copyright Act* provides the following definition of an intermediary: 29.21(1) “a person or entity who regularly provides space or means for works or other subject-matter to be enjoyed by the public.”⁵⁹²

Notice and Notice:

Notice and Notice provisions were introduced into the copyright regulation scheme by Bill C-11, the *Copyright Modernization Act*.⁵⁹³ The Bill introduced ss. 41.25 and 41.26 which provides that an

⁵⁹⁰ Online: <http://laws-lois.justice.gc.ca/eng/acts/c-42/>

⁵⁹¹ Copyright Act (R.S.C., 1985, c. C-42), Sec. 2.4(1)(b). Added by S.C. 1997, c. 24, s.2.

⁵⁹² Copyright Act, Sec. 29.21(2).

⁵⁹³ Canada, Bill C-11, An Act to amend the Copyright Act, 1st Sess, 41st Parl, 2012, cl 47 (royal assent on 29th June 2012). A similar notice and notice scheme operated informally in Canada for many years before it was formalized through the 2012 amendments. See SOCAN at para. 110.

owner of copyright can send a notice to the ISP claiming infringement, the ISP will then locate the specific subscriber and relay the notice to the individual.

The intended role of the intermediary (the ISP) in these provisions is to pass on the notice. The intermediary is defined as:

“The person who provides the means, in the course of providing services related to the operation of the Internet or another digital network, of telecommunication through which the electronic location that is the subject of the claim of infringement is connected to the Internet or another digital network.”⁵⁹⁴

3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
- Depends on the commercial or for-profit nature or intent of the use or user;
- Is uncertain and, if so, why;
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

For all of the following answers the provisions on infringement apply. The *Copyright Act* provides in section 27(1) that “it is an infringement of copyright for any person to do, without the consent of the owner of the copyright, anything that by this Act only the owner of the copyright has the right to do.” The ignorance or good faith of the infringer is irrelevant. For example in an earlier decision, *Compo Co. v. Blue Crest Music Inc.*, which concerns the pressing of records without consent of the copyright holder the Supreme Court found that the fact that the infringer was unaware that the owner of copyright had not consented was irrelevant.⁵⁹⁵ The absence of commercial use is also irrelevant to a finding of infringement.⁵⁹⁶ However, commercial infringers face more stringent civil liability and criminal penalties.

a) Downloading copyright-protected content from illegal/unauthorized sources on the Internet.

Downloading copyright protected content from illegal/unauthorized sources is illegal according to s. 3(1) of the *Copyright Act* which protects the rights of the copyright holder to produce or reproduce the work:

“For the purposes of this Act, *copyright*, in relation to a work, means the sole right to produce or reproduce the work or any substantial part thereof in any material form whatever, to perform the work or any substantial part thereof in public or, if the work is unpublished, to publish the work or any substantial part thereof.”

This reproduction right includes translation rights to (a) make any sound recording, (d) rent out a computer program, (h) rent out the sound recording, (i) amongst others.

⁵⁹⁴ The Copyright Act, Sec. 41.25(a).

⁵⁹⁵ [1980] 1 S.C.R. 357, at 375 per Estey J.

⁵⁹⁶ See *Bishop v. Stevens*, [1990] 2 S.C.R. 467, at 480; and *Compo Co. v. Blue Crest Music Inc.*, *supra*, at 375.

One exception to this rule stems from the private copying regime under Part VIII of the Act. Section 80(1) of the Act provides that the copyright in a musical work, performer's performance, or sound recording is not infringed by a person reproducing a musical sound recording onto an audio recording medium for the private use of the person who makes the copy. This user right in relation to musical sound recordings makes no reference to the provenance of the musical work, and so is theoretically available to one who makes a copy of an infringing reproduction, for example by downloading a musical sound recording through an unauthorized peer-to-peer network. The musical sound recording private copying exception is distinct from the general exception to copying for "personal purposes" contained in s. 29.22(1), which requires the source copy to have been non-infringing and legally made.

b) Streaming copyright-protected content from illegal/unauthorized sources on the Internet.

Streaming from illegal/unauthorized sources for private viewing is not illegal. The Supreme Court of Canada has sharply distinguished between reproductive activities (resulting in a multiplication of copies) and performance activities (which are experiential in nature) in its interpretation of the legislation. In *Rogers Communications Inc. v. Society of Composers, Authors and Music Publishers of Canada*,⁵⁹⁷ the Court confirmed that the right to communicate to the public contained in section 3(1)(f) of the *Copyright Act* is a technologically neutral species of performance right which includes both "push" and "pull" transmissions, but does not include transmissions initiated for the purposes of downloading a more or less permanent copy (implicating the reproduction right).

Online streams accordingly engage one of the "performance" rights. Over the internet, this would involve a communication. A party making a work available to others to stream may violate s. 3.1(f)'s communication right (communication of the work to the public by telecommunication) and its included making available right. However, merely experiencing the work in private implicates no rights: such private performances are not captured by the owner's rights in the legislation. The provenance of the stream has no bearing on the legality of the act. Since the Act does not grant copyright owners an exclusive right of private performance, the reception or viewing of a stream from even an unlawful source would not infringe.

It could be argued that streams involve reproductions (in the form of RAM copies or copies made for technical purposes) and hence potentially infringe the reproduction right. However, even if such temporary copies could be said to be sufficiently fixed to attract copyright, the Act includes in s. 30.71 an exception for liability for such reproductions where an essential part of a technological process to facilitate a non-infringing use.⁵⁹⁸ This provision is yet to be judicially interpreted by the courts. The language is not specific as to whose infringing use disqualifies the exception. I think the user still gets the benefit of the exception because of the way the court has fundamentally divided user rights under the Act between performance rights and reproduction rights. Streaming is a performance by virtue of its experiential nature, not because of the technical application of this exception benefiting reproductions for technical purposes. The party making content available to be streamed will be liable for reasons that have nothing to do with this particular user's activities.

The Act also protects intermediaries from liability in these contexts: merely providing storage does not infringe. Pursuant to section 31.1(4) of the *Copyright Act*, "a person who, for the purposes of allowing the telecommunication of a work or other subject-matter through the Internet, *provides digital memory in which another person stores the work does not, by virtue of that act alone, infringe copyright in the work.*"

⁵⁹⁷ 2012 SCC 35.

⁵⁹⁸ Sec. 30.71 reads: "It is not an infringement of copyright to make a reproduction of a work or other subject-matter if: (a) the reproduction forms an essential part of a technological process; (b) the reproduction's only purpose is to facilitate a use that is not an infringement of copyright; and (c) the reproduction exists only for the duration of the technological process."

c) Stream-ripping copyright-protected content.

The legality of stream-ripping has not yet been addressed by the Courts in Canada. It is likely that stream ripping content will be considered a breach of copyright through the *Copyright Act* provisions concerning reproduction of copyrighted material (section 3(1)(d)). See answer to question 3(a) above.

It is also possible to consider stream-ripping to be a circumvention of a technological protection measure. Canada's anti-circumvention provisions have yet to be considered by an upper level court. Lower courts have been incredibly generous to both the interpretation of "technological protection measure"⁵⁹⁹ and "circumvention"⁶⁰⁰. Where ripping a stream involves descrambling a scrambled signal or decrypting an encrypted signal, liability surely follows.⁶⁰¹ Where ripping a stream involves an act to "avoid, bypass, remove, deactivate or impair" a technological protection measure, liability will also follow.⁶⁰² However, it is too early in the history of the anti-circumvention scheme to state with certainty the nature of acts that fall within and without the broader aspects of the definition of circumvention.

d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.

Section 3(1) sets out the exclusive rights to produce or reproduce a copyrighted work held by a copyright holder. Uploading content to a website or online platform involves a reproduction that would constitute a prima facie infringement. However, these rights include the right to authorize the use of the work. The Supreme Court addressed whether the transmission of a work was a reproduction in *Rogers Communications Inc. v. Society of Composers, Authors and Music Publishers of Canada*.⁶⁰³ It confirmed that the right to communicate to the public contained in section 3(1)(f) of the *Copyright Act* is a technologically neutral right that covers both push and pull on demand streams, but does not cover downloaded copies (which would implicate the reproduction right) (per majority).

A party making a work available to others to stream, in contrast, may violate s. 3.1(f)'s communication right (communication of the work to the public by telecommunication) and its included making available right.

On the Court's interpretation, an unauthorized party uploading content to a publicly accessible website will infringe the reproduction right (since the party has made an unauthorized reproduction on the website's server), and the right of communication to the public by telecommunication (since the act involves making available to the public unauthorized content. A member of the public streaming such content for private performance purposes will not infringe the reproduction or the communication right.

The *Copyright Act* provides for an exception in relation to "Non-commercial user-generated content." Section 29.21 provides: "It is not an infringement of copyright for an individual to use an existing work or other subject-matter or copy of one, which has been published or otherwise made available to the public, in the creation of a new work or other subject-matter in which copyright subsists and for the individual" for non-commercial purposes.

⁵⁹⁹ A small claims court has found that a simple "paywall" comprising a simple username and password qualifies: 1395804 Ontario Limited (Blacklock's Reporter) v Canadian Vintners Association, 2015 CanLII 65885 at para. 52 (ON SCSCM), <http://canlii.ca/t/glmsq>.

⁶⁰⁰ Acquiring an unauthorized reproduction from one authorized to access the work behind a paywall amounts to circumvention: *ibid.*

⁶⁰¹ Copyright Act, Sec. 41(a).

⁶⁰² *Ibid.*, Sec. 41(a) and (b).

⁶⁰³ 2012 SCC 35.

In addition there are limited fair dealing user rights which may allow a work to be uploaded to a website or online platform (often not in full), these include research, education, parody or satire.⁶⁰⁴ The Supreme Court has found that the fair dealing purposes “must be given a large and liberal interpretation in order to ensure that users’ rights are not unduly constrained.”⁶⁰⁵

The Federal Court has recently adopted a stricter interpretive approach regarding fair dealing. In 2017, the Court held that for fair dealing to cover parody in uploading copyrighted content online, the court must be satisfied there is any intent for humour.⁶⁰⁶ A notice of appeal has been filed for this case.

e) Posting **hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.**

- *Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard **surface hyperlink**, **deep-link**, **embedded or framing hyperlink**).*

The courts have only addressed the issue of hyperlinks in the context of the law of defamation. In *Crookes v. Newton* the Supreme Court addressed, defamation which requires a publication, finding that a hyperlink is not by itself a publication of the content to which it refers.⁶⁰⁷ Rather the reference must be used in a way that itself conveys defamatory meaning. In coming to this conclusion, the court spoke on the importance of hyperlinks to facilitate access to information on the internet, per Abella J:

“The Internet cannot, in short, provide access to information without hyperlinks. Limiting their usefulness by subjecting them to the traditional publication rule would have the effect of seriously restricting the flow of information and, as a result, freedom of expression. The potential “chill” in how the Internet functions could be devastating, since primary article authors would unlikely want to risk liability for linking to another article over whose changeable content they have no control. Given the core significance of the role of hyperlinking to the Internet, we risk impairing its whole functioning. Strict application of the publication rule in these circumstances would be like trying to fit a square archaic peg into the hexagonal hole of modernity.”⁶⁰⁸

Based on this approach, Canadian commentators have doubted that hyperlinks, by themselves, constitute a copyright infringement.

f) The sale of **Kodi boxes or similar devices.**

There is currently an injunction against the sale of set-top boxes in Canada. The legality of them will be determined at trial in *Bell Canada v. 1326030 Ontario Inc. (iTVBox.net)*.⁶⁰⁹ The trial has still not yet been scheduled. In the case the plaintiffs, tel-co companies (Bell Media Inc., Rogers Media Inc., and Groupe TVA Inc.), applied for and got an injunction against the defendants who were individuals and businesses that sell set-top boxes. Plaintiffs claimed that the defendants were carrying or inducing copyright infringement through the manufacture and sale of these set-top boxes. Only one of the five defendants appeared at the injunction hearing. The defendant (business name: MtlFreeTV.com) argued that the set-top boxes were simply hardware in the same way as a tablet or a computer, that there is no doctrine of inducement in Canadian copyright law, and that there is no direct link between the sale of the set-boxes and the reduction in subscribers to the tel-co.’s services.

⁶⁰⁴ The Copyright Act at Sec. 29.

⁶⁰⁵ *CCH Canadian Ltd. v. Law Society of Upper Canada*, 2004 SCC 13 (CanLII), at para. 51.

⁶⁰⁶ *United Airlines, Inc v Cooperstock*, 2017 FC 616 (CanLII), < <http://canlii.ca/t/h4jzk> > at para 123.

⁶⁰⁷ See *Crookes v. Newton*, 2011 SCC 47, [2011] 3 SCR 269.

⁶⁰⁸ *Crookes v. Newton*, 2011 SCC 47, [2011] 3 SCR 269, at para 36.

⁶⁰⁹ 2016 FC 612 (CanLII), <<http://canlii.ca/t/gv257>>.

The findings made by the court include: The devices marketed, sold and programmed by the Defendants enable consumers to obtain unauthorized access to content for which the Plaintiffs own the copyright. All of the defendants market themselves as being plug and play. Beyond this the legal uses of set-top boxes are many and that is something to be determined at the trial stage. In the meantime the judge was satisfied that the applicants had established a strong prima facie case of copyright infringement and that an injunction would prevent irreparable harm without unduly inconveniencing the Defendants. An appeal from this decision in 2016 was unsuccessful.⁶¹⁰ In 2018, the Defendant was charged with contempt of Court for continuing to sell a set-top box after the issued injunction.⁶¹¹

The Federal Court of Appeal has also partially relied on this decision to order an injunction against the TVAddons websites, which offered services “no different from the service offered through the set-top boxes.”⁶¹²

g) Other types of unauthorized online use of copyright-protected content not listed above.

Section 29.22 of the *Copyright Act* (on “reproduction for private purposes”) introduced a private copying exception: it is not an infringement of copyright for an individual to reproduce a work or other subject-matter or any substantial part of a work or other subject-matter if:

- “ (a) the copy of the work or other subject-matter from which the reproduction is made is not an infringing copy;
- (b) the individual legally obtained the copy of the work or other subject-matter from which the reproduction is made, other than by borrowing it or renting it, and owns or is authorized to use the medium or device on which it is reproduced;
- (c) the individual, in order to make the reproduction, did not circumvent, as defined in section 41, a technological protection measure, as defined in that section, or cause one to be circumvented;
- (d) the individual does not give the reproduction away; and
- (e) the reproduction is used only for the individual’s private purposes.”

This general private copying exception is not remunerated. However, the specific private copying regime for musical sound recordings (sections 79 et seq.) is balanced by a right to remuneration in the form of a levy applied to blank audio recording media used for this purpose.

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

No. The *Copyright Act* does not differentiate.

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country’s law? If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.

Liability exceptions for intermediaries are contained in the *Copyright Act*.

2.4(1)(b)⁶¹³ to the *Copyright Act* which provides that persons who only supply “the means of telecommunication necessary for another person to so communicate” are not themselves to be considered parties to an infringing communication.

⁶¹⁰ *Wesley (Mtlfreetv.com) v. Bell Canada*, 2017 FCA 55 (CanLII), <<http://canlii.ca/t/h2tnt>>.

⁶¹¹ *Bell Canada v. Vincent Wesley dba MtlFreeTV.com*, 2018 FC 66 (CanLII), <<http://canlii.ca/t/hqf5p>> at para 93.

⁶¹² *Bell Canada v Lackman*, 2018 FCA 42 (CanLII), <<http://canlii.ca/t/hqj8w>> at para 35.

More specifically the *Copyright Modernization Act* introduced safe harbor provisions for intermediaries (that essentially codify the Supreme Court cases discussed below). The relevant sections are 31.1(1)-(2),(4); 41.27(1).

Key case on intermediaries and the internet:

*Society of Composers, Authors and Music Publishers of Canada v. Canadian Association of Internet Providers.*⁶¹⁴ In *SOCAN* the court looked at copyrighted musical works that were transmitted over the internet. The Society of Composers, Authors, and Music Publishers of Canada sought to impose liability for royalties on various internet service providers (ISP) for the transmission of these works. The court considered the extent to which the ISP's were aware of the content shared and their role as a conduit of content. It concluded that an intermediary as a content provider does not lose the protection of paragraph 2.4(1)(b) by "providing their normal facilities and services, such as housing and maintaining the servers, and monitoring "hits" on particular Web pages, because these added services are merely ancillary to the provision of disk space and do not involve any act of communication."⁶¹⁵ The majority held further that the location of the host server does not matter (*i.e.* if it is in Canada versus overseas).⁶¹⁶

Search engine:

In *SOCAN* the Supreme Court of Canada clarified that S. 2.4(1)(b) shields intermediaries from liability (see above). In this decision the court took a broad approach to the meaning of telecommunication, including all "connection equipment, connectivity services, hosting and other facilities and services." It is likely that search engine fits within this definition.

See para 92:

"Section 2.4(1)(b) shields from liability the activities associated with providing the means for another to communicate by telecommunication. "The 'means'", as the Board found, "... are not limited to routers and other hardware. They include all software connection equipment, connectivity services, hosting and other facilities and services without which such communications would not occur" (p. 452). I agree. So long as an Internet intermediary does not itself engage in acts that relate to the content of the communication, *i.e.*, whose participation is content neutral, but confines itself to providing "a conduit" for information communicated by others, then it will fall within s. 2.4(1)(b). The appellants support this result on a general theory of "Don't shoot the messenger!"

The most pertinent decision related to search engines is *Century 21 Canada Limited Partnership v. Rogers Communications Inc.*, a 2011 decision.⁶¹⁷

In *Century 21* the defendants Zoocasa, a subsidiary of Rogers, indexed in full house listings created by Century 21. The Court found that these listings were copyrighted works. The matter was decided on contract principles, the court found that Zoocasa was in breach of Century 21's terms of use which prohibited a user from copying or reproducing content. The court did not consider s.2.4(1)(b) and the role of the search engine broadly through the lens of it being an intermediary activity. Importantly the search engine created and utilized by Zoocasa is to be distinguished from other generic search engines (such as google) as it was a vertical search engine designed specifically to locate and access information about real estate listings. Based on this, the excerpt from *SOCAN* above remains the most relevant legal finding on search engines.

⁶¹³ Copyright Act (R.S.C., 1985, c. C-42), Sec. 2.4(1)(b). Added by S.C. 1997, c. 24, s.2.

⁶¹⁴ 2004 SCC 45. [*SOCAN*]

⁶¹⁵ *SOCAN*, at para. 103.

⁶¹⁶ *SOCAN*, at para. 106.

⁶¹⁷ 2011 BCSC 1196 (CanLII), <<http://canlii.ca/t/fn00h>>. [*Century 21*].

An Ontario court has recently held that this shelter extends to intermediaries providing tools to locate information, and does not extend to a provider that gathers information from the Internet and makes it available on their own website.⁶¹⁸ The appeal was dismissed.⁶¹⁹

User generated content:

The *Copyright Act* provides for an exception in relation to “Non-commercial user-generated content.” Section 29.21 provides: “It is not an infringement of copyright for an individual to use an existing work or other subject-matter or copy of one, which has been published or otherwise made available to the public, in the creation of a new work or other subject-matter in which copyright subsists and for the individual” for non-commercial purposes.

In the context of provisions concerning user generated content the *Copyright Act* provides the following definition of an intermediary: 29.21(1) “ a person or entity who regularly provides space or means for works or other subject-matter to be enjoyed by the public.”⁶²⁰

Notice and Notice:

Notice and notice provisions were introduced into the copyright regulation scheme by Bill C-11, the *Copyright Modernization Act*.⁶²¹ The Bill introduced ss. 41.25 and 41.26 which provides that an owner of copyright can send a notice to the ISP claiming infringement, the ISP will then locate the specific subscriber and relay the notice to the individual.

The intended role of the intermediary (the ISP) in these provisions is to pass on the notice. The intermediary is defined as:

“The person who provides the means, in the course of providing services related to the operation of the Internet or another digital network, of telecommunication through which the electronic location that is the subject of the claim of infringement is connected to the Internet or another digital network.”⁶²²

If the intermediary did not pass on the notice to the subscriber at the identified IP address they are subject to fines.⁶²³

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

No

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These

⁶¹⁸ *Trader Corp v CarGurus Inc*, 2017 ONSC 1841 (CanLII), < <http://canlii.ca/t/h32jb>> at para 46.

⁶¹⁹ *CarGurus, Inc v Trader Corporation*, 2017 FCA 181 (CanLII), < <http://canlii.ca/t/h5t20>>.

⁶²⁰ The Copyright Act, Sec. 29.21(2).

⁶²¹ Canada, Bill C-11, An Act to amend the Copyright Act, 1st Sess, 41st Parl, 2012, cl 47 (royal assent on 29th June 2012). A notice and notice scheme operated informally in Canada for many years before it was formalized through the 2012 amendments. See SOCAN at para. 110.

⁶²² The Copyright Act, Sec. 41.25(a).

⁶²³ The Copyright Act, Sec. 41.26(3).

measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:

- The suspension from the Internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.
- The monitoring or **filtering** of content.
- The **blocking** and removing of infringing content, including notice-and-takedown.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- **Graduated response systems.**

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

The *Copyright Act*'s remedial provisions are general in nature, and generally do not depend on the nature of the protected content.

a) Civil.

The *Copyright Act* imposes civil liability on users who (i) infringe copyright and (ii) circumvent technological protection measures ("TPMs").

In copyright infringement proceedings, copyright owners are entitled to all remedies conferred by law for the infringement of a right, including injunction, damages, and accounts.⁶²⁴ Instead of actual damages, owners may elect to recover statutory damages, capped at \$20 thousand for commercial infringements and \$5 thousand for all non-commercial infringements.⁶²⁵

Sub-section 40(1) limits remedies available for copyright infringements involving the construction of a building or other structure. The successful copyright owner is not entitled to obtain an injunction in respect of the construction or to order its demolition, or to recover possession of infringing copies or "plates" (*i.e.*, blueprints) used to produce such copies.

Copyright owners can also launch civil proceedings against users who circumvent TPMs contrary to s.41.1(1)(a). In circumvention proceedings, rights holders are entitled to the full range of remedies available in infringement proceedings. However, statutory damages cannot be awarded against an individual who circumvented TPMs only for his or her own private purposes.

b) Administrative.

⁶²⁴ The Copyright Act, Sec. 34(1).

⁶²⁵ The Copyright Act, Sec. 38.1(1).

The Act includes separate statutory damages provisions in cases involving non-payment of royalties where the Copyright Board has approved a tariff. Sub-section 38(4) provides that where a defendant has not paid applicable royalties, a collective society may recover an award of statutory damages in a sum of not less than three and not more than ten times the amount of the applicable royalties.

c) Criminal.

The *Copyright Act* criminalizes both copyright infringements and circumventions of TPMs for commercial purposes.⁶²⁶ Offenders are liable: (a) on conviction on indictment, to a fine of not more than \$1 million or to imprisonment for a term of not more than five years or to both; or (b) on summary conviction, to a fine of not more than \$25 thousand or to imprisonment for a term of not more than six months or to both.⁶²⁷

The Criminal provisions of s. 42 are not applicable to infringers involving the construction of a building or other structure: see s. 40(2).

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law against intermediaries to address online copyright infringement by third party users of their services?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

The *Copyright Act*'s remedial provisions are general in nature, and generally do not depend on the nature of the protected content.

a) Civil.

Intermediary safe harbours:

The *Copyright Act* shelters most internet intermediaries, such as ISPs, hosting services, and search engines, from civil liability for copyright infringement by their users.⁶²⁸

Enabler liability:

The so called "enabler" provision, section 27(2.3) of the *Copyright Act*, creates an exception to the general intermediary safe harbour. The enabler provision makes it an infringement of copyright to provide a service primarily for the purpose of enabling acts of copyright infringement if an actual infringement of copyright occurs as a result of the use of that service. The "enabler" provisions would be the main tool available to copyright holders to attack internet intermediary services such as the Pirate Bay or Popcorn Time. Indeed, this was one of the bases of the lawsuit filed by Music Canada against isoHunt Web Technologies Inc. and Gary Fung (isoHunt offered a bittorrent search service).⁶²⁹ The provision has yet to be interpreted by a Canadian court,

The *Copyright Act* includes a similar provision that prohibits providing services or manufacturing technology primarily for the purposes of facilitating the circumvention of TPMs.⁶³⁰

Notice-and-notice regime:

⁶²⁶ The Copyright Act, Secs. 42(1), 42(3.1).

⁶²⁷ The Copyright Act, Sec. 42(2.1).

⁶²⁸ The Copyright Act, Secs. 2.4(1)(b), 31.1(1)-(2),(4), 41.27(1).

⁶²⁹ B.C. Sup. Ct. File No. S086309, settled on consent July 13, 2016.

⁶³⁰ The Copyright Act, Secs. 41(1)(b)-(c).

Notice-and-notice is a ‘made in Canada’ solution to online copyright infringement. In force since 2015, the notice-and-notice system empowers copyright holders to discourage online copyright infringement. First, the copyright holder will notify the relevant ISP to allege infringement on the ISP’s network. This notice will include the IP address linked to the alleged infringement. Then, the ISP will find the specific subscriber and relay the notice. The subscriber’s personal information is not divulged to the copyright holder.

The *Copyright Act* requires that ISPs forward notices to their subscribers and retain records for a limited time. A claimant’s only remedy against an ISP who fails to perform their obligations is statutory damages capped at \$10 thousand.

Norwich orders:

Copyright holders can ask a court to identify alleged infringers through an equitable bill of discovery, also known as a Norwich order. If the court agrees, it can compel a non-party intermediary to share the subscriber’s details.

b) Administrative.

N/A

c) Criminal.

N/A

9. To the best of your knowledge, are there significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

We know of no significant differences in public and private enforcement practices. Individual copyright owners behave differently from one another, but these differences do not describe the industry as a whole.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

Without a court order (view Norwich order above), intermediaries do not have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holder. Disclosure of this information would contravene Canada’s federal privacy legislation, the Personal Information Protection and Electronic Documents Act (“PIPEDA”).

a) If yes, what conditions must be met for that obligation to arise?

Section 7(3) of PIPEDA allows disclosure of personal info without knowledge or consent, by an organization, if required by a court-issued order. In order to obtain a Norwich order against an intermediary, the applicant must demonstrate:

- (a) a valid, bona fide or reasonable claim;
- (b) that the intermediary is somehow involved in the acts complained of;
- (c) that the intermediary is the only practicable source of the information; and
- (d) that the interests of justice favour the obtaining of disclosure from the intermediary.

*see Norwich order case law listed in question 12 (b) of this survey

b) If yes, what type of personal data is typically requested?

In Norwich order motions, rights holders typically request the disclosure of subscriber information (names and addresses) linked to allegedly infringing IP addresses. This disclosure allows rights holders to pursue litigation against the alleged infringer.

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

The *Copyright Act* grants standing to the owner of any copyright, or any person deriving any right, title or interest by assignment from the owner, to protect and enforce any right they hold and entitles them to the remedies provided by the Act.⁶³¹ Exclusive licensees may similarly exercise such rights. Non-exclusive licensees and sole licensees, in contrast, may not.

Copyright collectives have standing under the legislation to enforce payment of royalties under an approved tariff or agreement: *Copyright Act*, para. 34(4)(c). They may exercise such right regardless of the mechanism by which they are authorized to act: assignment, grant of licence, appointment as agent or otherwise, the form of authorization to collectively administer copyright does not matter (see definition of “collective society”, s. 2).

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

- Please indicate whether the measures refer to public or private enforcement.

(i) Infringement notices (private enforcement):

The most common enforcement measure against infringing users is infringement notices sent by right holders via intermediaries. While there are no comprehensive statistics on Canada’s notice-and-notice system, copyright holders have sent millions of notices since the law came into force in early 2015.

Canadian Intellectual Property Rights Enforcement (“Canipre”), a company that sends copyright infringement notices on behalf of copyright holders, said it sent out more than six million notices in 2015. Canipre says it has provided rights holders with more than \$500 thousand from people who have accepted a settlement.

Copyright infringement notices are sent in Canada both through the notice and notice system, and by way of Norwich orders, third party discovery orders obtained by copyright owners by way of application to court to require ISPs to provide the applicant with the identity and addresses of subscribers associated with certain IP addresses alleged to be involved in infringing internet communications. Notices sent through the notice and notice system have no need for the ISP’s subscriber information, and may work anonymously by threatening legal action if the recipient does not get in touch with the copyright owner. These often direct recipients to enter their information on a webform, or pay a “settlement fee” online. Such forms can be very intimidating, threatening legal consequences. In some cases, notice senders have alleged infringement of US laws with much steeper damage claims. Such notices arguably abuse the notice and notice provisions.

(ii) Infringement and anti-circumvention civil proceedings (private enforcement):

⁶³¹ The Copyright Act, Sec. 41.23(1).

Generally speaking, rights holders have not launched many civil infringement and anti-circumvention proceedings against users and intermediaries. In the few proceedings before Canadian courts, rights holders have pursued Norwich orders against ISPs, injunctions against sellers of infringing or circumventing technology, and in one unique case, the certification of a reverse class action against multiple non-commercial infringers. These cases are explored below in question 12 (b).

(iii) Criminal investigations (public enforcement):

Despite criminal provisions in the *Copyright Act*, there have been very few examples of public copyright enforcement in Canada.

- a) Were any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?**

(i) Infringement notices (private enforcement):

The notice-and-notice provisions of the *Copyright Act* came into force at the start of 2015, however there was an informal warning system between rights holders and ISPs in place prior to the formal provisions.

(ii) Infringement and anti-circumvention civil proceedings (private enforcement):

The 2012 copyright amendment created new provisions for civil liability that have been used over the last three years. The amendment introduced civil liability for circumventing TPM's and also included the 'enabler' provision, which makes it a copyright infringement to provide a service or manufacture a technology primarily for the purpose of enabling acts of copyright infringement.

(iii) Criminal investigations (public enforcement):

Despite new criminal provisions for the circumvention of TPMs included in the 2012 copyright amendment, there has not been an increase in criminal enforcement of copyright.

- b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.**

(i) Infringement notices (private enforcement)

N/A

(ii) Infringement and anti-circumvention civil proceedings (private enforcement)

Anti-circumvention:

Nintendo of America Inc v King, 2017 FC 246: Court finds defendant's 'mod chips' circumvented Nintendo's TPMs and infringed copyright. Court awards Nintendo \$11.7 million in statutory damages for anti-circumvention, \$60 thousand in statutory damages for copyright infringement, \$1 million in punitive damages, delivery up of the defendant's inventory, and injunctions against the defendant's service.

Norwich Orders:

BMG Canada Inc v John Doe, 2005 FCA 193: Court of appeal upholds refusal to grant Norwich order requiring a group of ISPs to identify alleged infringers of BMG's copyright. Not enough evidence presented to show a bona fide claim of infringement.

Voltage Pictures LLC v Untel, 2011 FC 1024: Court grants Norwich order requiring a group of ISPs to identify alleged infringers of Voltage's copyright on the film *Hurt Locker*.

Voltage Pictures LLC v John Doe, 2014 FC: Court grants Norwich order requiring ISP TekSavvy to identify some 2000 alleged infringers of Voltage's copyright

Voltage Pictures LLC v John Doe No 1, 2016 FC 881: In a novel 'reverse class action' proceeding against a class of alleged infringers of Voltage's copyright, court grants Norwich order requiring ISP Rogers communication to identify the proposed class defendant. On appeal of the order, the court clarified that ISPs must maintain records in a manner that allows it to identify suspected infringers, and must pay the cost associated with transmitting those records.⁶³² It is yet to be determined whether the court will certify this novel class action proceeding.

Kodi Boxes:

Bell Canada v 1326030 Ontario Inc, 2016 FC 612: Court grants sweeping injunction against several distributors of television set-top boxes preloaded with software such as Kodi (plus addons), Showbox, or private IPTV services. The Federal Court of Appeal upholds the injunction (*Wesley v. Bell Canada*, 2017 FCA 55). A trial date has still not been scheduled.

(iii) Criminal investigations (public enforcement)

In 2016, US authorities shutdown Kickass Torrents and arrested the alleged founder following an investigation. Canadian authorities reportedly cooperated in the effort.

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

Abuse of the notice-and-notice system:

Certain groups of rights holders, sometimes referred to as 'copyright trolls', misuse the notice-and-notice regime to convey inappropriate settlement demands to vulnerable consumers in an effort to recover payments without litigation. The demands often include misleading legal information and obfuscate the unproven nature of these allegations. Canadians scared by the demands pay the settlements without ever being proven guilty.

Canadian civil society advocates are urging the Government to curb notice-and-notice misuse by implementing regulations that stipulate what may be included in a forwarded infringement notice.

Does Canada need stricter copyright enforcement laws?

Major rights holder groups in the US are asking Canada to create a stricter copyright enforcement regime. In their report to the US Trade Representative, the International Intellectual Property Alliance calls for strengthened legal incentives for ISPs to co-operate with rights holders, and for Canadian authorities to make online copyright enforcement a priority.⁶³³

On the other hand, some Canadian commentators say that recent court decisions show that Canada is already home to some of the toughest anti-piracy rules in the world. Moreover, the Business Software

⁶³² *Voltage Pictures LLC v John Doe No 1*, 2017 FCA 97 (CanLII), <<http://canlii.ca/t/h3s49>>.

⁶³³ <http://www.iipawebsite.com/rbc/2017/2017SPEC301CANADA.PDF>.

Alliance reports that Canada is at its lowest software-piracy rate ever, well below global and European averages.

Canadian copyright reform on the way?

Heading into 2019, two forums are set to impact Canadian copyright law. The first is a statutorily mandatory five year review of the *Copyright Act* which has recently begun. The review will consult witnesses from specific sectors of activity, a range of stakeholders and communities, and legal experts.⁶³⁴ The Government is aiming to complete the review by early 2019.

The second forum is the renegotiation of the North American Free Trade Agreement (“NAFTA”). The US have already stated that they will seek to strengthen international property laws as part of the renegotiation. It is likely that online copyright enforcement will be part of these discussions. These negotiations are ongoing.

Copyright web-blocking proposal

FairPlay Canada, a coalition led by telecom Bell, sought support from the Canadian Radio-television and Telecommunications Commission (CRTC) to implement a copyright web-blocking mechanism. The proposed Internet Piracy Review Agency (IPRA) would be an independent, third-party agency, enforced by the CRTC, and operate under the *Telecommunications Act* SC 1993, c38.

The proposal garnered considerable attention and backlash. The CRTC has received over 10,000 submissions in relation to the proposal, and a decision regarding its implementation has not yet been made.

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions/campaigns aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

Where to watch in Canada (www.wheretowatchincanada.ca):

This website, co-developed by the Motion Picture Association - Canada and the Canadian Media Production Association, aggregates legal online streaming and download to own services available to Canadian users.

Respect Copyright in Canada (www.respectcopyrightincanada.ca):

This website, developed by Motion Picture Association - Canada, provides an FAQ to users who have received infringement notices from their ISP.

Notice and Notice Regime FAQ (www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02920.html):

This federal government website provides factual information on the notice-and-notice regime and contains specific information for consumers who have received infringement notices.

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

No.

⁶³⁴ <<http://www.ourcommons.ca/DocumentViewer/en/42-1/INDU/news-release/9752040>>.

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

The lack of data related to online copyright infringement in Canada makes it difficult to track the effectiveness of various policies.

One potential area of study is Canada's notice and notice regime. Rights holders and ISPs are under no obligations to publish data on the number infringement notices they send and receive. This information would be useful for tracking alleged infringements and could be a useful tool to combat copyright trolls.

Questionnaire Hong Kong

ALICE LEE, Associate Dean (Academic Affairs) and Associate Professor, Faculty of Law, The University of Hong Kong

Last updated: 31 May 2018

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded **red**.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.

Civil liability of online copyright infringement is mainly created under the Hong Kong Copyright Ordinance (Cap. 528) (the “**HK Ordinance**”).

Criminal liability of online copyright infringement is mainly regulated under the HK Ordinance. There are also criminal liability provisions regulating the use of computers under the Hong Kong Crimes Ordinance (Cap. 200) (the “**Crimes Ordinance**”).

2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?

There is no specific definition of “intermediary” in the HK Ordinance.

There are no provisions in the HK Ordinance that define intermediaries or categorise intermediaries into different types.

3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
- Depends on the commercial or for-profit nature or intent of the use or user;

- Is uncertain and, if so, why;⁶³⁵
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

a) Downloading copyright-protected content from illegal/unauthorized sources on the Internet.

Downloading may attract civil liability under the HK Ordinance.

- Downloading from illegal or unauthorized sources qualifies as copyright infringement under the HK Ordinance. Since the downloader reproduces the copyright-protected content
- Civil liability does not depend on knowledge of the downloader.
- Civil liability may be influenced by the purpose or context of use. Under s.38-39, 41 and 41A of the HK Ordinance, the downloader may invoke a defence to infringement if the downloader can establish fair dealing for the purpose of research, private study, criticism, review, news reporting or education, and satisfy the specific acknowledgment and content removal requirements therein.
- Civil liability does not generally depend on the type of downloaded content.

Downloading may also attract criminal liability under the HK Ordinance.

- Downloading a copy may result in the downloader “possessing” an infringing copy of the work, which may potentially attract criminal liability under s.118(1)(f) or 118(2A) of the HK Ordinance.
- Criminal liability depends on the downloader’s knowledge. Under s.118(3) of the HK Ordinance, it is a defence for the person charged to prove that he did not know and had no reason to believe that the copy in question was an infringing copy of the copyright work. Note, however, that Hong Kong case law indicates that the downloader has the duty to make reasonable inquiries to make out this defence (*Infabrics Ltd v Jaytex Ltd* [1980] 1 Ch 282, applied in *R v Ng Kwan Pui* [1988] HKC 724 and *HKSAR v Mega Laser Products (HK) Ltd* [1999] 3 HKC 161)
- Criminal liability depends on the purpose/context being in the course of trade or business.
 - Under s.118(1)(f), the prosecution has to prove that the possession is with a view to the infringing copy either (1) “being sold or let for hire by any person for the purpose of or in the course of any trade or business”, or (2) “being exhibited in public or distributed by any person for the purpose of or in the course of any trade or business which consists of dealing in infringing copies of copyright works”.
 - Similarly, under s.118(2A), the prosecution has to prove that the possession is with a view to the infringing copy “being used by any person for the purpose of or in the course of any trade or business”.
- Criminal liability does not generally depend on the type of downloaded content.

b) Streaming copyright-protected content from illegal/unauthorized sources on the Internet.

Streaming alone, without more, is unlikely attract civil liability under the HK Ordinance:

- For the end-user who streams from illegal or unauthorized sources, he/she is unlikely to attract civil liability as streaming by itself is not covered by any of the exclusive acts defined in s.22 of the HK Ordinance.
- Nonetheless, civil liability may still arise if the streamed content is then played in public or broadcasted (e.g. a restaurant playing streamed content) as it would then be covered under one of the exclusive acts in s.22 of the HK Ordinance.

⁶³⁵ For instance: the act is not clearly covered by exclusive rights, may be covered by an exception or limitation, may be subject to implied consent, the illegal/unauthorized nature of the source is unclear, or other.

Streaming only attracts criminal liability under limited circumstances under the HK Ordinance.

- Streaming by itself is unlikely to attract criminal liability because it is not covered by any of the offences specified in ss.118(1) or 118(2A). Moreover, in contrast to the civil liability position, even if the streamed content is played in public or broadcasted, the legal position re criminal liability is still uncertain. The issue is whether the act of streaming music/audio files for performance would mean that the streamer “distributes an infringing copy of the work” under s.118(1)(f)(ii) or (g) of the HK Ordinance. One hurdle to establishing “distribution” is that even when played or broadcasted in public, the receiving end never receives a physical infringing copy through the streaming.
- Regardless of the above, criminal liability may arise if the streamed content is accessed by using IP address masking tools or VPNs. The masking of IP address to access jurisdiction-specific content may constitute use of computers with dishonest intent, and contravene s.161 of the Crimes Ordinance.

The discussion on knowledge, purpose/context of use, type of content in the **downloading** section applies equally to streaming (insofar as the streaming constitutes infringement).

c) Stream-ripping copyright-protected content.

See above discussion on **downloading**.

Under the law of Hong Kong stream-ripping does not constitute circumvention of TPMs.

d) **Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.**

Uploading is likely to attract civil liability under the HK Ordinance.

- Uploading is likely to infringe the “making available” right of the copyright holder under s.22(1)(d) & 26 of the HK Ordinance (i.e. “the making available of copies of the work, by wire or wireless means, in such a way that members of the public in Hong Kong or elsewhere may access the work from a place and at a time individually chosen by them”). There is no known definitive ruling on the civil liability of uploaders in Hong Kong to date.
- Civil liability does not depend on the uploader’s knowledge.
- Civil liability may be influenced by the purpose or context of use. The discussion on fair dealing in the **downloading** section is equally applicable here.
- Civil liability does not generally depend on the type of uploaded content.

Uploading is also likely to attract criminal liability under the HK Ordinance:

- Uploading infringing content to online platforms falls within the definition of “distribut[ion]” under ss.118(1)(f)(ii) and 118(g) of the HK Ordinance. This is so regardless of whether the uploader uploads the entire file onto a publicly accessible cyberlocker, or whether the uploader merely uploads a seed file (see *HKSAR v Chan Nai Ming* (2007) 10 HKCFAR 273).
- Criminal liability depends on the uploader’s knowledge under s.118(3). The discussion in **downloading** on knowledge is equally applicable here.
- The purpose or context of use affects whether the element of “prejudice to the copyright owner” has to be proven to establish criminal liability. Under s. 118(1)(g) of the HK Ordinance, if the distribution is otherwise than for the purpose of or in the course of any trade or business which consists of dealing in infringing copies of copyright works, then the prosecution is required to prove that the uploading is to such an extent as to affect prejudicially the copyright owner. Under *HKSAR v Chan Nai Ming* (2007) 10 HKCFAR 273, the threshold is very low: the prejudice to be proven is not necessarily restricted to economic prejudice, and even small losses in sales may be sufficient to amount to prejudice. In contrast, if the uploading is “for the purpose of or in the course of any trade or business which consists of dealing in infringing copies of copyright works”, then there is no need for the prosecution to prove prejudice.

- Criminal liability does not generally depend on the type of uploaded content.
- e) **Posting hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.**
 - *Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard surface hyperlink, deep-link, embedded or framing hyperlink).*

There is no known ruling in Hong Kong as to the status of hyperlinking to date.

Hyperlinking is likely to attract civil liability under the HK Ordinance:

- Hyperlinking may be covered by the “making available” right under s.26 of the HK Ordinance. Under s.26 of the HK Ordinance, civil liability may arise since the alleged infringer “makes available” copies of the work to the public. Note, however, that there is no definitive case law on this point to date.
- For hyperlinking activities that aim to circumvent technological measures in place, the hyperlink-poster may infringe s.273B(1) of the HK Ordinance, by providing a relevant service to circumvent technological measures.

Hyperlinking may attract criminal liability under the HK Ordinance, though the position is far from certain due to the lack of case law.

- Hyperlinking may possibly be an offence under s.118(1)(e) and (g) of the HK Ordinance. This depends on the HK Court’s interpretation as to whether the hyperlink-poster either “*exhibits in public an infringing copy of the work*” or “*distributes an infringing copy of the work*”. The difficulty in establishing criminal liability re hyperlinking under s.118 is two-fold: (i) in hyperlinking, there is no “infringing copy” per se, and (ii) the end-consumers who click on the hyperlink does not receive a permanent infringing copy (without further action, the contents in the link may only be stored temporarily in the browser cache file).
- For hyperlinking activities that aim to circumvent technological measures in place (e.g. password restrictions, restricted user access), the hyperlink-poster would infringe s.273C(1) of the HK Ordinance, by providing a relevant service to circumvent the measures put in place by the website operator.

f) The sale of Kodi boxes or similar devices.

There is a no known ruling in Hong Kong as to the status of the sale of Kodi boxes/similar devices.

Kodi box sellers may attract civil liability under one the following heads:

- Infringement by authorisation under s.22(2) of the HK Ordinance – in *Moorhouse and Angus & Robertson (Publishers) Pty v University of New South Wales* [1976] RPC 151, 165 (applied in Hong Kong in *Sky King Machinery Engineering Ltd v Chun Wo Construction & Engineering Co Ltd* [2015] HKEC 400), it is held that a person who has under his control the means by which an infringement may be committed, who makes it available to other persons, having reason to suspect that it is likely to be used for infringement purposes without taking reasonable steps to limit its use would be held to be authorising an infringement. Thus, if reasonable steps are not taken by Kodi box devices which have technological measures that enable users to circumvent paywalls, there is a risk that the seller or manufacturer may infringe by authorisation.
- Contributory infringement by common design – similarly, it might be held that the Kodi box sellers would be jointly and severally liable for the infringements committed by its users if the seller intends and procures and shares a common design that infringement shall take place (*CBS Songs Ltd v Amstrad Consumer Electronics Plc* [1988] RPC 567 at 578).
- By allowing the user to circumvent technological measures in place, the Kodi box seller or manufacturer may infringe s.273B(1) of the HK Ordinance by selling a relevant device that is either primarily designed or adapted for enabling or facilitating the circumvention of the measure,

or has been promoted for the purpose of circumvention of the measure, or has only a limited commercially significant purpose other than circumvention of measure.

Kodi-box sellers may also attract criminal liability under s.273C(1) of the HK Ordinance

- By selling the Kodi box itself, Kodi box sellers are unlikely to attract liability under s.118 of the HK Ordinance if the device does not download/reproduce any infringing copy and only enables user to stream from online sources.
- However, if there are no in-built security devices to prevent technological circumvention of viewing restrictions, or if the seller “jail-broke” the security devices of the streamed sources within the Kodi-box, then the Kodi box may constitute a relevant device that aim to circumvent technological measures. This means that the seller and manufacturer may contravene s.273C(1) of the HK Ordinance.

g) Other types of unauthorized online use of copyright-protected content not listed above.

Nothing to report.

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

There is no specific difference between minors and adults in the context of finding liability for copyright infringement.

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country’s law? If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.

There is no intermediary-specific liability exemption or safe harbor available under the HK Ordinance.

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

The extent of involvement required to establish liability remains uncertain. Under Hong Kong law, there are two main routes to establish liability of online intermediaries: (i) infringement by authorisation under s.22(2) of the HK Ordinance, or (ii) contributory infringement as a common law tort. Both require a heavily fact-sensitive inquiry as to whether there are any measures in place to enforce the takedown of infringing contents, the main activities of the online intermediary etc. Due to the absence of case law and the limited guidance in the HK Ordinance, there is uncertainty as to (i) what are the factors by which the Hong Kong Courts would infer authorisation or contributory infringement, and (ii) the relative weight to be attributed to each factor.

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:

- The suspension from the internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.
- The monitoring or filtering of content.
- The blocking and removing of infringing content, including notice-and-takedown.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- Graduated response systems.

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

As to civil remedies directed at the direct infringer:

- Injunctions (e.g. take-down orders)
- Damages
- Account of profits

Section 107 of the HK Ordinance provides that

- (1) An infringement of copyright is actionable by the copyright owner.*
(2) In an action for infringement of copyright all such relief by way of damages, injunctions, accounts or otherwise is available to the plaintiff as is available in respect of the infringement of any other property right.

Section 108 further provides that

- (1) Where in an action for infringement of copyright it is shown that at the time of the infringement the defendant did not know, and had no reason to believe, that copyright subsisted in the work to which the action relates, the plaintiff is not entitled to damages against him, but without prejudice to any other remedy.*
(2) The court may in an action for infringement of copyright having regard to all the circumstances, and in particular to-
(a) the flagrancy of the infringement;
(b) any benefit accruing to the defendant by reason of the infringement; and
(c) the completeness, accuracy and reliability of the defendant's business accounts and records, award such additional damages as the justice of the case may require.

b) Administrative.

Nil.

c) Criminal.

Under s.119 of the HK Ordinance, the infringer who committed an offence under s.118 of the HK Ordinance may be liable on conviction on indictment to a fine at level 5 in respect of each infringing copy and to imprisonment for 4 years. The current level 5 fine is defined in Schedule 8 of the Criminal Procedure Ordinance (Cap. 221) as HK\$ 50 thousand.

Moreover, under s.161 of the Crimes Ordinance, a person who accesses computer with criminal or dishonest intent may be liable on conviction upon indictment to imprisonment for 5 years.

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law against intermediaries to address online copyright infringement by third party users of their services?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

Depending on the degree of involvement of the online intermediaries and whether any measures are taken to ensure the removal of infringing content, online intermediaries may be liable for infringement by authorisation or contributory infringement. In such circumstances, the civil remedies are as follows:

- Injunctions and takedown orders
- Damages
- Account of profits

Please note that these remedies are the same as identified above in the answer to Question 7.a).

Where the degree of involvement of online intermediaries is insufficient to find liability, injunctions may be available against the online intermediaries, which may include:

- Takedown orders against forums
- Website blocking orders against ISPs
- De-indexing orders against indexing and bookmarking sites (including search engines)

De-indexing orders and website blocking orders have not been tested before the Hong Kong Courts, although it is expected that the Hong Kong Courts would largely follow the approach in England under its wide powers to grant injunctive relief.

b) Administrative.

Nil.

c) Criminal.

Nil.

9. To the best of your knowledge, are there significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

No known differences based on the type of protected content between public and private enforcement practices.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

a) If yes, what conditions must be met for that obligation to arise?

A Norwich Pharmacal application may be made to compel the disclosure of the personal data of alleged infringers by an online intermediary. The conditions for an applicant (usually the copyright owner) invoking Norwich Pharmacal discovery are as follows:

- Serious tortuous or wrongful activities had been committed;
- The alleged wrongdoer was a person whom the applicant bona fide believed to be infringing his rights in the sense that he could reasonably be assumed to be the wrongdoer vis-à-vis the applicant; and
- The innocent party, against whom discovery was sought, had been caught up or had become involved in such activities, thus facilitating the perpetration or continuation of the same.
- It is just and convenient in all the circumstances of the case for the court to exercise its discretion to grant the relief. This usually means that the scope of disclosure must be necessary, proportionate and justified.

b) If yes, what type of personal data is typically requested?

Typically, the IP address of the user, name, contact details of the user would be requested. These details enable the copyright owner to take action against the relevant persons. For instance, in *Cinepoly Records Co Ltd v Hong Kong Broadband Network Ltd* [2006] 1 HKC 433, music producers asked the ISPs to disclose the names, addresses and HK ID card numbers of persons who allegedly uploaded infringing files through a P2P file sharing programme (WinMX).

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

For civil relief:

- The copyright owner (including the assignee – see ss. 103(1) & 112(1) of the HK Ordinance) has standing to sue in court. Note that an equitable assignee has to join the legal owner before final relief can be obtained (*Takmay Industrial Co Ltd v Wah Sang Industrial Co* [1977-79] HKC 115)
- The exclusive licensee, after joinder with the copyright owner (see s.113 of the HK Ordinance)

For criminal liability:

- Criminal proceedings are usually formally instituted by the Prosecutions Division of the HKSAR Department of Justice. Nonetheless, the investigation and arrest stage is usually carried out by the Hong Kong Customs and Excise Department.
- Private prosecutions are possible, but are rarely ever invoked in Hong Kong.

No criminal offenses for copyright infringement are ‘private crimes’ or ‘complaint-based’ (i.e. its not a requirement for prosecution of the offence that the aggrieved party files a complaint).

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

- Please indicate whether the measures refer to public or private enforcement.

Private: Takedown notices issued to local and foreign online intermediaries (i.e. in the context of notice-and-takedown systems voluntarily set-up by online intermediaries).

Private: Infringement notices issued to alleged infringers (and court actions, e.g. injunction, upon non-compliance)

Public: Reporting to and cooperating with Customs and Excise Department in enforcement actions, mainly through the Intellectual Property Rights Protection Alliance

a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?

They are mainly matters of practice rather than measures in national law.

b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.

In terms of public enforcement, the Hong Kong Customs and Excise Department have recently relied on the LMSI+ system to monitor popular online forums in Hong Kong and to track and arrest uploaders of audio-visual contents. These cases typically involve uploading and distribution of infringing copies through using cyberlockers: the uploaders would first upload an infringing copy to a cyberlocker, and then post hyperlinks that lead to the cyberlocker on a popular forum. By tracking the posts on popular online forums using the LMSI+ system, several people were arrested.

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

In terms of private enforcement, there were discussions as to the implementation of an intermediaries' safe harbor and notice-and-takedown regime in Hong Kong. However, the bill to implement such a regime was voted against by the Legislative Council in 2016. There are no known plans by the current administration to re-commence the implementation.

In terms of public enforcement, there are controversies raised by Pan-Democratic legislators and local netizens as to the possible abuse of s.161 of the Crimes Ordinance (access to computers with dishonest intent) in tackling online crimes. Their main concern is that the use of this route may suppress freedom of expression.

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions/campaigns aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

The Intellectual Property Department in Hong Kong hosts regular talks and workshops to educate the public on IP issues generally. Some of the talks may touch upon online copyright infringement.

The Customs and Excise Department also operates the Youth Ambassador Against Internet Piracy Scheme to cooperate with local youth uniform organisations to combat illegal peer-to-peer file sharing activities using BT. This is part of the Intellectual Property Rights Protection Alliance initiative, which aims to establish cooperation between the Customs and Excise Department with right-holders and businesses in Hong Kong.

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

There are two main issues:

- Jurisdictional and choice of law issues involved in online copyright enforcement, especially when the infringers involve a group of companies utilizing the services of online intermediaries located in other jurisdictions (e.g. the PRC, USA);
- The prevalent use of VPNs, browser plugins and other IP address-masking tools in order to circumvent geographical restrictions in the viewing of copyright-protected contents. As a sinophone city, Hong Kong citizens have limited linguistic barriers in viewing copyright-protected contents from PRC websites. Although the PRC websites and intermediaries have tried to enforce copyright protection by mandating the implementation of geographical restrictions, VPNs and other plugins allow the circumvention of such restrictions with relative ease.

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

As to data on enforcement statistics, the Customs and Excise Department is mainly responsible for regulating such activities. However, the statistics published on the website does not suggest a very clear distinction between cases involving offline articles and online takedowns. Separate data sets may have to be directly requested from the Department.

Questionnaire Indonesia

Dr. HENRY SOELISTYO, S.H., LL.M, Head, Master and Doctor of Law Program, Universitas Pelita Harapan. Jakarta

Last updated: 28 May 2018

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded red.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.

- Law No. 28 Year 2014 on Copyright (**Copyright Law**).

From the WIPO website (<http://www.wipo.int/wipolex/en/details.jsp?id=15600>):

“On September 16, 2014, the Indonesian Parliament passed Law No. 28 of 2014 on Copyright. It exempts the non-commercial reproduction and distribution of copyrighted materials through information and technology media from the scope of the authors’ exclusive rights. In the enforcement area, it prescribes the concept of landlord liability under which a landlord or the manager of a building is liable to criminal penalties if they know that a tenant carries out copyright-infringing activities and gives the Ministry of Communication authority to remove copyright-infringing websites.

The Law also introduces mandatory mediation and arbitration procedures for certain types of infringement, extends the scope of acts liable for criminal enforcement, and increases the level of criminal sanctions.”

The provision that exempts the non-commercial reproduction and distribution of copyrighted materials through information and technology media from the scope of the authors’ exclusive rights is Article 43d of the Copyright Act, which reads: “...Manufacture and distribution of copyright content through information and communication technology that is not commercial and/or beneficial for Author or related parties, or Author expressed no objection to the said manufacture and dissemination.”

- Law No. 11 Year 2008 on Information and Electronic Transaction (**ITE Law**).
- **Joint Regulation** of Minister of Law and Human Rights No. 14 Year 2015 and Minister of Communication and Information No. 26 Year 2015 on *Implementation of Content Closing and/or Access Right of Users of Copyright Infringement and/or Related Rights in Electronic System*.

The Joint Regulation (in force since 2 July 2015) implements sections of the Copyright Law 2014 which make illegal online content that infringes copyright. This was set up as joint regulation because the responsibility on copyright administration and enforcement is held by those two institutions. The Ministry of Law and Human Rights (and its Directorate General of IP –DGIP) has overall responsibility for copyright issues, whereas the blocking of online access is only possible technically done by the Ministry of Information and Communication.⁶³⁶

- **Circular Letter No. 3 Year 2016** of the Minister of Information and Communication concerning *Service Provider Application and/or Content through Internet (Over the Top)*.
- **Circular Letter No. 5 Year 2016** of the Minister of Information and Communication concerning *Limitation and Accountability of Trade Platform Provider through Electronic System (Electronic Commerce)*.

2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?

Intermediary is recognized in national law as an independent legal entity that engages in the field of internet service provider. Some are state-owned enterprises (such as Telkom Indonesia and Indosat), and others are private companies. National law does not differentiate the notion or specific types of intermediaries, such as dialup, DSL, cable, wi-fi access, and satellite. All these are defined in Article 1 number 6, Article 15 and Article 16 ITE Law as the electronic system provider. This ITE Law regulates, among others, electronic system provider, its operation and the responsibility of electronic system provider.

3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
- Depends on the commercial or for-profit nature or intent of the use or user;
- Is uncertain and, if so, why;
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

As a preliminary remark, Indonesian Copyright Law sets the copyright infringement norms broadly. The violation covers all kinds of reproduction in any manner and in any forms, both permanently and temporarily (Article 1 number 12 of Copyright Law 2014). Besides, the violation of performing right covers all forms of performing by using any means so that the creation can be read, heard, or seen by other persons (Article 1 Point 11 of Copyright Law 2014).

⁶³⁶ Although this system operated under the 2008 ITE Law regulations “and has been widely used against pornography, it is now specifically targeting copyright infringements. It wasn’t clear how IP violations which were referred to in the 2008 [ITE Law] were supposed to be treated.” See <http://ipkomododragon.blogspot.nl/search/label/Indonesia%20copyright?updated-max=2015-09-09T23:58:00-07:00&max-results=20&start=10&by-date=false>)c

a) Downloading copyright - protected content from illegal / unauthorized sources on the Internet.

Specifically, a downloading action is qualified as a violation of Copyright, not based on the downloaded source (whether the source is illegal/unauthorized or a legal source) but determined based on whether there is a license or an approval or not. The mechanism of approval from the copyright owner can be given through a direct license or using a mechanism of license based on collecting management organization system/CMO.

As indicated in Article 113 para 1,2,3 jo. Article 9 para 1 Copyright Act, categorization as copyright infringement does not depend on knowledge or awareness of the users, particularly on matters relating to the illegal/unauthorized status of sources. However, that matter is more based on intention, that is, if done for commercial purpose or for profit nature. The concept of categorization as a basis for exception or fair dealings clause is defined in Article 46, which reads as follows:

(1) Reproduction for personal interest to a work on which Announcement has been conducted, can only be made in 1 (one) copy and can be done without the permission of the Author or the Copyright Holder.

(2) Reproduction for personal interest referred to in subsection (1) does not include:

- a. works of architecture in the form of a building or other construction;*
- b. the whole or a substantial part of a book or musical notation;*
- c. the whole or a substantial part of the database in digital form;*
- d. Computer programs, except as referred to in Article 45 paragraph (1); and*
- e. Reproduction for personal interests whose execution is in conflict with the reasonable interests of the Creator or the Copyright Holder.*

The other acts would be exempted based on the principle of fair use or fair dealing. The same clause prevailed in the previous Copyright Act No. 19 Year 2002.

Meanwhile, reproduction of work (moving or transferring) in a form of downloading the content protected by Copyright, by law, is included in the category of torts (Article 30 Para (2) ITE Law). So, both Copyright Act and Torts are applicable for court proceeding.

In sum, downloading copyright-protected content from illegal / unauthorized sources on the Internet is illegal unless it is made for non-commercial purposes, in which case it will be considered to be for “personal interest” and covered by the exception or fair dealings defense in Article 46.

b) Streaming copyright-protected content from illegal/unauthorized sources on the Internet.

According to Copyright Law 2014, streaming is included in the coverage of publication or performance. These concepts are defined in Article 1 number 11 concerning publications and **number 12 concerning reproduction**. Such action is deemed as a copyright infringement if without any permit from the creator of work.

If the streaming material is a news item, then the streaming action is not considered as copyright infringement if done for non-commercial purposes. This is regulated in the provision regarding exceptions or limitations (Article 43 letter d Copyright Law 2014). In this context, an act which is not considered a violation of Copyright include: “...(d) manufacture and distribution of copyright content through information and communication technology that is not commercial and/or beneficial for Author or related parties, or Author expressed no objection to the said manufacture and dissemination.”

[Clarification by national expert: Article 43 letter d Copyright Law 2014 applies to all types of copyright-protected content. The reason why the streaming of “news” is not considered to be an infringement is because current news is only protectable for 3x24 hours (elucidation of copyright

law). If the news is taken during that period solely for non-commercial purpose, it is deemed as not infringement]

Streaming as a performance is also a forbidden act. (Article 30 Para (2) ITE Law), if committed from an unauthorized source to do the content's copyright transmission (Article 32 number (1) ITE Law).

c) Stream-ripping copyright-protected content.

As noted above, Indonesian Copyright Law sets the copyright infringement norm broadly. The violation covers all kinds of reproduction in any manner and in any forms, both permanently and temporarily (Article 1 number 12 of Copyright Law).

With such a broad norm as defined in Copyright Law 2014, the stream-ripping copyright protected content can be categorized as copyright infringement, as such stream-ripping is factually and technically similar to reproduction. Such action is not considered as copyright infringement if not for commercial purposes (Article 46).

Stream-ripping action is deemed online copyright infringement if towards transmission copyrighted content, the temporarily downloaded file (temporary reproduction) is saved and has its form changed into a file that is able to re-duplicate permanently. Such process can damage the function of content securing system which means a violation of technological measures (Article 52 of Copyright Law and Article 30 Para (3) of ITE Law).

d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.

Without authorization of the author or right holder, uploading copyright protected content constitutes an infringement. Article 9 Para (1) Copyright Law determines that right of communication and performance is an exclusive right of the copyright holder.

The action of electronic information and/or electronic document transfer to anyone who has no right, including conducting communication, sending, and broadcasting of such electronic information is considered prohibited in Article 32 number (2) of ITE Law.

Technically, the uploading action is included in the scope of reproduction as regulated in Copyright Law. The law defines the terms “ ... in any forms,” which means it also covers the change of recording from physical format (compact disc/video compact disc/digital video disc) into the MP3 digital format, waveform audio format (WAV), MP4, or change from book into an audio book (Article 1 number 12, Article 9, elucidation of Article 24 letter d of Copyright Law).

e) Posting hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.

- Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard surface hyperlink, deep-link, embedded or framing hyperlink).

The usage of hyperlinks that contains of copyright content is not considered as violation of Copyright. The reason is because such hyperlink only mentions the URL address from the relevant copyright content. There is no reproduction or action of making such copyright works available to the public.

There is no reported case on this issue.

f) The sale of Kodi boxes or similar devices.

Copyright law does not specify the sale of Kodi boxes or similar devices as copyright infringement. However, the ITE Law regulates the prohibition of selling, producing, distributing, providing, or owning such **device to facilitate unlawful acts** (Article 34 number (1) of ITE Law). **These unlawful acts are specified below but it should be noted that none of them refers to copyright infringement.**

Article 34 ITE Law, stipulates specific provision as follows:

Any Person who intentionally and without right or unlawfully produces, sells, causes to be used, imports, distributes, provides, or owns:

Computer hardware or software that is designed or specifically developed to facilitate actions meant in Article 27 to Article 33

Computer Passwords, Access Codes, or the like which are intended to cause the Electronic System accessible with the purpose to facilitate actions as meant in Article 27 to Article 33.

For further clarification, the cited provisions on prohibited acts are as follows:

Article 27 ITE Law:

- (1) Any Person who intentionally and without right distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents which have contents that are contrary to morality.*
- (2) Any Person who intentionally and without right distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents which have contents on gambling*
- (3) Any Person who intentionally and without right distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents that have contents of insult and/or defamation*
- (4) Any Person who intentionally and without right distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents which have contents of extortion and/or threat*

Article 28 ITE Law:

- (1) Any Person who intentionally and without right disseminates false and misleading information which results in consumer's loss in Electronic Transaction*
- (2) Any Person who intentionally and without right disseminates information aimed at inflicting hatred or creating hostility of individuals and/or certain groups of people based on ethnicity, religion, race, and inter-group*

Article 29 ITE Law:

Any Person who intentionally and without right sends Electronic Information and/or Electronic Document which contain threat of violence or to scare which is intended personally

Article 30 ITE Law:

- (1) Any Person who intentionally and without right or unlawfully accesses Computer and/or Electronic System owned by other Person in any ways*
- (2) Any Person who intentionally and without right or unlawfully accesses Computer and/or Electronic System in any ways with the purpose to acquire Electronic Information and/or Electronic Document*
- (3) Any Person who intentionally and without right or unlawfully accesses Computer and/or Electronic System in any ways by violating, hacking into, trespassing into, or breaking through the security system.*

Article 31 ITE Law:

- (1) *Any Person who intentionally and without right or unlawfully carries out interception or tapping of Electronic Information and/or Electronic Documents in certain Computers and/or Electronic System owned by other Person*
- (2) *Any Person who intentionally and without right or unlawfully carries out interception or transmission of Electronic Information and/or Electronic Document that are not of public nature from, to, and within a Computer and/or certain Electronic System owned by other Person, whether or not causing alteration, deletion, and/or termination of Electronic Information and/or Electronic Document that are being transmitted.*
- (3) *Exempted from interception as meant in paragraphs (1) and (2), interception that is carried out for law enforcement upon request of police, prosecutor, and/or other institutions whose authorities are determined by the law.*
- (4) *Further provisions on procedures of interception as meant in paragraph (3) shall be regulated by Law.*

Article 32 ITE Law:

- (1) *Any Person who intentionally and without right or unlawfully in any manner alters, adds, deducts, transmits, destroys, deletes, moves, hides, Electronic Information and/or Electronic Document owned by other Person or public*
- (2) *Any Person who intentionally or without right or unlawfully in any manner moves or transfers Electronic Information and/or Electronic Document to Electronic System of other unauthorized Person*
- (3) *Towards the actions meant in paragraph (1) which cause the confidential Electronic Information and/or Electronic Document to be revealed, that it becomes accessible to public with the wholeness of data that is not supposed to be.*

Article 33 stipulates that:

Any Person who intentionally and without right or unlawfully carries out any actions that cause the disturbance of Electronic System and/or cause Electronic System not working properly as supposed to be.

There is no reported case on this issue.

g) Other types of unauthorized online use of copyright-protected content not listed above.

No relevant information available.

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

Not specifically. However, the procedure and accountability would be different. Parents and guardian are responsible for the damage caused by the minors who live with them, and upon whom they are acting the parental or guardianship authority (1367 Civil Code). For copyright infringement done by minors, the settlement is processed in the special juvenile court, while adults shall be in the district court.

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country's law?⁶³⁷ If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.⁶³⁸

At the moment, it is debatable whether online intermediaries benefit from liability exemption. However, Article 1367 Indonesia Civil Code indicates that the intermediaries have liability based on duty of care principle. The full text of the article is the following:

⁶³⁷ For example, in the EU, Arts 12 to 14 of the E-Commerce Directive include conditional liability exemptions (regarding claims for damages) to the benefit of intermediaries concerning the provision of services of 'mere conduit', 'caching', and 'hosting'.

⁶³⁸ For instance: to what type of services they apply and subject to which conditions.

A person is responsible for the damage which was caused by his own act, as well as for that which was caused by the acts of the individuals for whom he is responsible, or caused by matters which are under his supervision.

Parents and guardians are responsible for the damage caused by minor children who live with them and over whom they exercise parental authority or guardianship.

Employers and those who have appointed others to manage their affairs are responsible for the damage caused by their servants and subordinates in the course of the duties assigned to them.

Teachers and craftsmen are responsible for the damage caused by their students and apprentices, during the period the latter are under the formers' supervision.

The above- mentioned responsibilities cease, if the parents, guardians, school teachers and work supervisors can prove that they were unable to prevent act, for which they would be liable.

In addition, Article 56 of Criminal Code stipulates a principle as follows:

The person is deemed as accomplices to a crime shall be punished in certain condition when he/she:

- 1. deliberately aid in the commission of the crime*
- 2. deliberately provide opportunity, means, or information for the commission of the crime*

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

Since Indonesia has no ISP Liability Act, then there is no regulation on liability of intermediaries. However, the activities of ISP and other service providers are regulated in the following Circular Letters of the Minister of Information and Communication.

- **Circular Letter No. 3 Year 2016** concerning Service Provider Application and/or Content through Internet (Over the Top)
 - This Circular Letter, among others, regulates the obligation to obey the IPR laws and broadcasting and film regulation.
- **Circular Letter No. 5 Year 2016** concerning Limitation and Accountability of Trade Platform Provider through Electronic System (Electronic Commerce).
 - In this circular letter the prohibition of content publication that violates IPR is clearly stipulated.
 - Besides that, the platform provider has the obligation to determine the requirement of platform usage, including provisions regarding the responsibility of uploaded content.
 - Platform provider also has the obligation to provide embedded means of reporting that is used to deliver complaints towards illegal contents in its managed platform.
 - Towards the complaint received, the platform provider has the obligation to conduct obliteration or blocking of such illegal contents, including illegal copyrighted works.
 - If the platform provider does not comply with such obligation, then the Ministry of Communication and Information will close it.

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by

intermediaries to prevent or end infringement are:

- The suspension from the internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.
- The monitoring or filtering of content.
- The blocking and removing of infringing content, including notice-and-takedown.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- Graduated response systems.

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

As a preliminary remark, there are no differences depending on the type of protected content.

a) Civil.

Civil laws can be applied towards online copyright infringement cases, both through amicable settlement (out of court) and through court settlement, especially via commercial court. The main purpose of taking these measures is to acquire remedies (civil remedies).

Copyright Law also provides mechanism of injunction (Article 106) to stop the violation actions. Article 106 Copyright Law stipulates specific rules of injunction (Anton Pillar Order) with the following procedure:

At the request of those who feel aggrieved because of the Copyright or Related Rights enforcement, the Commercial Court may issue provisional measures for the purpose of:

- preventing the entry of goods suspected of infringing the Copyright or related rights into the trade channel;
- withdrawing from the circulation/distribution and seizing and storing as evidence related to the infringement of Copyright or Related Rights;
- securing evidence and preventing the obliteration by the offender; and / or
- stopping the violation in order to prevent greater damage.

Note that Anton Pillar Orders can apply to online infringement cases.

In addition, the Copyright Law stipulates a process of proof of evidence by using electronic information and/or electronic document (Article 111 of Copyright Law).

b) Administrative.

Administrative procedure is governed by the **Joint Regulation** of Minister of Law and Human Rights and Minister of Communication and Informatics regarding the *actions upon online traffic with warning letters and further actions in a form of site blocking*. The power is based on Article 55 Copyright Law:

- (1) *Every person who knows copyright infringement and/or related rights through electronic system for Commercial Use can report to the Minister*
- (2) *The Minister shall verify the report as meant in paragraph (1)*
- (3) *In case of insufficient evidence based on the results of verification of report as meant in paragraph (2), upon request of the complainant, Minister shall recommend to the Minister who carries out governmental affairs in the field of telecommunication and informatics to cover part of all contents that infringe Copyright in the electronic system or make the electronic system service cannot be accessed.*
- (4) *In the case of closure of Internet sites as meant in paragraph (3) conducted as a whole, within 14 (fourteen) days after the closure, the Minister shall request for a court decision.*

The Joint Regulation stipulates a procedure of complaints related to online copyright and/or related rights infringement reported either directly to Ministry of Communication and Informatics or to the Ministry of Law and Human Rights. Complaints could be submitted by any copyright holder including author, licensee or CMO on behalf of the author and/or songwriters. Any complaint could be made to the DGIP directly or through an electronic system. In this respect, e-complaints can be submitted via the DGIP website. Administratively, a verification team at the Ministry of Communication and Information goes through reports and provide recommendations to Directorate General of Informatics. Decisions can be made to partly or entirely block access to infringing content. Blocking may be content or access blocking. There are a series of time limits and a public database of blocked sites/users.⁶³⁹

Specifically in the **Circular Letter of Minister of Communication and Information No. 5 Year 2016**, it is stipulated that UGC Platform Providers have an obligation to provide a reporting instrument that can be used to deliver complaints regarding prohibited contents in the managed platform to obtain specific link toward its prohibited content, including copyright. In this respect, based on the sufficient evidence, platform providers would take necessary action and block the access.

NB the Circular Letter and the Joint Regulation different operational instruments under the Copyright law and the ITE Law.

c) Criminal.

Maximum 4 years imprisonment and/or maximum 1 billion rupiah fine enforced on economic rights violation in a form of publication and duplication of works as well as distribution and announcement of works (Article 113 para (3) of Copyright Law).

The provision specifically defines that for economic right violation in a form of reproduction/duplication, is categorized as piracy of copyright works. The sanction for such piracy is determined heavier with maximum criminal imprisonment of 10 years and/or 4 billion rupiah fine. (equivalent to USD 296 thousand). By definition, Article 1 number 28 clarify the meaning of piracy as follows : Duplication or reproduction of copyright works and/or related right without license or illegal and distribution of such works massively in order to obtain economic benefit or profit.

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law against intermediaries to address online copyright infringement by third party users of their services?

- *When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).*

Basically there are no differences among the type of protected content.

⁶³⁹ See <http://ipkomododragon.blogspot.nl/search/label/Indonesia%20copyright?updated-max=2015-09-09T23:58:00-07:00&max-results=20&start=10&by-date=false>

a) Civil.

In civil procedures, liabilities are handed over to intermediaries because the principle of accountability for damages caused by the deed of persons under their responsibility or caused by properties under their supervision (Article 1367 of Civil Code). The procedure of settlement with third parties is not defined in the Copyright Law and ITE Law. Remedies of third party users' action in their services are determined based on the initial agreement regarding content and deeds that are considered violating the law. As indicated in the answer to Question 5, an online platform is liable for copyright infringement of its users. In this case the applicable enforcement measures are the same as for directly liable end users.

b) Administrative.

Joint Regulation No. 14 Year 2015 regulates also the accountability of intermediaries. The point is, its settlement is handed over to the discretion of intermediaries. In practice, it is done by sending a warning letter or through a termination of contract (such as blocking or deletion of content) with third parties. The remedies and sanctions are determined based on prevailing laws as well as administrative rules and regulation. Prevailing laws include contract law, company law, regulation on administrative license, including operational license.

In short, if a third party as a user is committing copyright infringement, the intermediaries will: 1) send such user a warning letter to stop infringement, and/or 2) terminate the contract with the user. In addition, it would be possible to suspend a user from access to the Internet while the Ministry of Communication and Informatics finalizing the evidence of the infringement.

c) Criminal.

If a criminal violation happens caused by a third party user, the intermediaries acting as their service provider (ISP, file hosting or other online media) can be criminally sanctioned based on Article 56 of Criminal Code on aiding the commission of crime (see answer to Question 5). The essence of violation is "giving opportunity or means before the crime happens."

It should be noted that this article has no definite sanction.

[Clarification by expert: Article 56 has no definite sanction in its text. However, the sanction is defined in article 57 that is counted one-third less from the primary punishment. If judge decide necessary, the additional punishment for intermediaries could be given equal to the punishment for the main actor of criminal action.]

Consequently, intermediaries will conduct necessary actions based on duty of care principle in following up the agreement with third party users of their services (their clients).

9. To the best of your knowledge, are there significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

There are no significant differences.

Please note that 2015 Indonesia established a government agency called the Creative Economy Industry Agency ("BEKRAF") to foster and grow the sector. One of the stated goals of the BEKRAF was to develop an "Online Anti-Piracy Alert System".

The Online Anti-Piracy Alert System is not yet operational. The BEKRAF started to set up a team with the Ministry of Justice and Ministry of Communication and Informatics.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

Yes, in accordance to the TRIPs Agreement in which Indonesia has to comply due to the membership of WTO. However this obligation has not been regulated in national law.

a) If yes, what conditions must be met for that obligation to arise?

So far there is no case, so that the individual data involved in copyright infringement has never been disclosed by the infringer. In this matter, it is assumed that such data is only limited to the main and relevant data to help the investigation of the copyright infringement case thoroughly. Accordingly, the disclosure could be made at the request of right holders.

b) If yes, what type of personal data is typically requested?

It is assumed that the relevant data only concerns the individual's identity, such as name, address, profession, and closest contact person. If there is a judicial court order, all related data could be disclosed.

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

Copyright holder and/or exclusive licensee regarding civil, administrative or criminal measures

In addition, CMOs can apply for enforcement measures covering administrative and criminal measures. Administrative measures under the Joint Regulation can only be pursued if there is first a complaint by the rights holder, licensee, or CMO.

Concerning the criminal system, Article 120 Copyright Law determines that copyright infringement is a complaint-based system.

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

- Please indicate whether the measures refer to public or private enforcement.

For public enforcement, it is common to go through the police report in accordance to the rules of criminal law system. If there is enough evidence, a copyright infringement case will be followed up by public prosecutors in order to be brought to the court.

From the side of private enforcement, an infringer can be sued in civil way for compensation and discontinuation of copyright infringement.

Copyright holder can also go through the settlement through Alternative Dispute Resolution.

Besides that, provisional measures (Anton Pillar Orders) can also be used for injunction relief, including in the case of online infringement. The procedure of measures is stipulated in the Supreme Court regulation. Another Supreme Court regulation governs the procedure of suspension of pirated product.

From the aspect of administrative law, it can be charged with site closure with the mechanism of reporting to Communication and Informatics Department according to the Circular Letter of Minister of Communication and Informatics No. 5 Year 2016.

a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?

Yes, regarding the administrative option of closing a website through the procedure of the Circular Letter of Minister of Communication and Informatics No. 5 Year 2016.

b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.

- Provisional measures being used to stop the circulation of Soekarno movie, and successfully approved by the Central Jakarta Commercial Court in 2014.⁶⁴⁰
- Closure of 21 internet sites by the Minister of Communication and Informatics based on the report from Aprofri (Association of Indonesian Movie Producers) in 2015.

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

Law enforcement, both private and public, encounters serious obstacle in facing *digital piracy* or *online copyright infringement*. Debates have gone for a long time, starting from the ineffectiveness of Copyright Law 2002 in preventing and overcoming a serious and massive digital piracy. Discussion is getting stronger when bill of the Copyright Law is being formulated, to replace Copyright Law 2002. The topic's approach covers three matters, which are legal substance, legal structure, and legal culture.

From the **substantive** aspect, many thoughts expect the Copyright Law to regulate more clearly and assertive the protection norms of Copyright in relation to the digital technology. One of the issues covers the meaning and scope of exclusive right that has to be clarified to cover protection over creations in digital media. In addition, the necessary legal norms for digital violation of copyright.

From the aspect of **legal structure**, the issue is in the understanding, both in the aspect of juridical normative, as well as from the aspect of technical knowledge related to the information technology.

Lastly, from the aspect of **legal culture**. The point is the honor culture, reward, protection of Copyright, is still low. People tend to ignore the legal responsibility to honor and protect others' Copyright, especially because there are many kinds of convenience in using others' creations through digital technology.

It should be acknowledged that the legal aspect itself until today is still problematic, even though in Copyright Law 2014, the norms of digital Copyright protection are already accommodated. The most important thing, in the 2014 Copyright Law, such norms of digital protection still have to be interpreted and not user-friendly. The lack of understanding is not only on legal aspects but also on technical matters.

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last

⁶⁴⁰ On which see <http://ipkomododragon.blogspot.nl/2014/01/indonesias-first-civil-search-and.html> and http://ipkomododragon.blogspot.nl/2015/03/trial-and-appeal-leaves-uncertainty_19.html

three years? If yes, were these actions/campaigns aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

In the last 3 – 5 years, online copyright infringement campaign has been done, such as seminar, discussions, and information campaigns. Besides that, the writing competition and musical show are done to voice out the meaning of piracy in Jakarta and other big cities. The purpose is to educate and increase the understanding, devoted to build the public awareness. Besides by the Government, cq Directorate General of Intellectual Property, seminar is also done by the private that is sponsored by associations/organizations of interest. Among others, organizations related to music, such as CMO and association of sound recording industry and movie. The target is the public at large and particularly for users of music, movie, books, and software. The advertisement of people's service also becomes the media campaign of anti-piracy by the related association and organization.

As reported by the media, there is new infringing website list made with the aim to reduce online piracy. The list which was originally initiated in the United Kingdom by the Police Intellectual Property Crime Unit being introduced in Indonesia involving the Creative Economy Agency (BEKRAF), the Indonesian Film Producers Association, Recording Company Association (ASIRI), Indonesian Association of Advertising Agencies and Motion Picture Association. The program focused to identify the most popular piracy websites in Indonesia and encourage advertiser to remove their ads from such websites. It was reported that piracy websites have caused musicians and music labels to suffer huge losses. So far more than 300 infringing websites on music were blocked.⁶⁴¹

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

Copyright Law 2014 does not regulate specifically the right of copyright holder to conduct legal action related to injunction, especially provisional measures towards intermediaries. Legal rules related to provisional measures only apply towards primary infringers.

One of the interesting cases is the making of music VCD by a company of Inul Vista's Singing who takes videos from the files available in Youtube. Such action is not considered by the court as online copyright infringement, especially Mechanical Rights. North Jakarta District Court Decision in May 2016 causes many critics and objections. Since the illegal practice is not classified as criminal action, then the decision becomes controversial. Because, the court only assesses that this problem is a private issue, that is, originating from non-fulfillment of musical creation duplication's license.

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

No, there is no statistical data regarding online copyright infringement.

⁶⁴¹ See <http://jakartaglobe.id/features/new-infringing-website-list-aims-to-reduce-online-piracy/> regarding a New Infringing Website List Aimed at reducing Online Piracy.

Questionnaire Japan

TATSUHIRO UENO, Professor of Law at Waseda University (Tokyo); Deputy Director of the Research Center for the Legal System of Intellectual Property (RCLIP) of Waseda University

Last updated: 27 May 2018

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded **red**.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.

Under the Japanese Copyright Act (1970),⁶⁴² copyright holders are granted the right of public transmission (Art.23(1)) against online copyright infringement.

2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?

There is no provision on “intermediary” in the Japanese Copyright Act. Additionally, there is no explicit provision under which a copyright holder may demand an injunction against a person who contributes to or supports another’s infringement in the Japanese Copyright Act.

The ISP Liability Limitation Act (Act No.137 of 2001)⁶⁴³ limits the liability for damages of ISPs (hosting providers), which applies not only to copyright infringement but also trade mark infringement, defamation and so on.

3. Does your national law qualify the following acts as copyright infringement?

⁶⁴² Translations of the Japanese Copyright Act are available at <<http://www.cric.or.jp/english/clj/>> and <<http://www.japaneselawtranslation.go.jp/law/detail/?id=1980&vm=2&re=&new=1>>. Regarding the outline written in English of the JCA and major cases, see Tatsuhiro Ueno, Chapter 22 (Japan) in: Silke von Lewinski (ed.) Copyright Throughout The World, (Thomson / West, loose-leaf from 2008); Teruo Doi / Tatsuhiro Ueno, Chapter JAPAN in: Lionel Bently (ed.), International Copyright Law and Practice (Matthew Bender/LexisNexis); Peter Ganeva / Christopher Heath / Hiroshi Saito (ed.) Japanese Copyright Law, Writings in Honour of Gerhard Schricker (Kluwer, 2005).

⁶⁴³ The translation is available at <<http://www.japaneselawtranslation.go.jp/law/detail/?id=2088&vm=02&re=01&new=1>>.

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content;
- Depends on the commercial or for-profit nature or intent of the use or user;
- Is uncertain and, if so, why;
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

a) Downloading copyright-protected content from illegal/unauthorized sources on the Internet.

Under the Japanese Copyright Act, downloading “digital sound or visual recording” from illegal or unauthorized sources, knowing that the recording is illegally uploaded without authorization, shall constitute copyright infringement, even if the downloading is conducted for private use (Art.30(1)(iii)). On the other hand, downloading contents other than sound or visual recording (e.g. PDF file, text file) shall not constitute copyright infringement under the Japanese Copyright Act, since the provision stipulates “digital sound or visual recording”.

b) Streaming copyright-protected content from illegal/unauthorized sources on the Internet.

Under the Japanese Copyright Act, streaming is basically not considered as reproduction in the meaning of the Copyright Act. Even in case a streaming causes a transient reproduction of a part of copyright-protected work (e.g. so-called progressive download), the reproduction shall be allowed as a reproduction required for the exploitation of works on computer, based on the explicit copyright exception (Art.47*octies*).

c) Stream-ripping copyright-protected content.

Stream-ripping causes a reproduction and downloading of the entire part of a copyright-protected work, in my understanding. Therefore, such stream-ripping is treated the same as downloading mentioned above (a).

In case such stream-ripping is made by the circumvention of “technological protection measures” which is defined in Article 2(1)(xx) of the Japanese Copyright Act and such reproduction is made by a person who knows the fact that such reproduction becomes possible by the circumvention of technological protection measures, the reproduction in the course of such stream-ripping shall constitute copyright infringement, even if the reproduction is conducted for private use (Art.30(1)(ii)).

d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.

Uploading copyright-protected content without authorization basically constitutes an infringement of the right of public transmission (Art.23(1)) under the Japanese Copyright Act.

e) Posting **hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.**

- Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard **surface hyperlink**, **deep-link**, **embedded or framing hyperlink**).

There are two court cases in Japan.

- In the Rocket News 24 Case, the Court, on 20 June 2013, held that embedding a movie that had been available on another video hosting platform (“Nikoniko-dôga”) did not amount to making available to the public of the work in the meaning of the Japanese Copyright Act.⁶⁴⁴
- In the Retweet Case, the Courts, on 15 September 2016 and on 25 April 2018, held that embedding a photo by way of the “retweet” by a twitter user that had been available as other person’s profile image in Twitter did not constitute a making available to the public of the work.⁶⁴⁵

However, this issue is still now under discussion in Japan. According to the major theories, posting hyperlinks even to illegal/unauthorized copyright-protected contents does not constitute a primary copyright infringement, because posting hyperlinks is not transmitting copyright-protected works to the public but just transmitting internet address (URL) of the works to the public.

On the other hand, posting hyperlinks to illegal/unauthorized copyright-protected contents can constitute a tort as a secondary liability under the Japanese Civil Code, because it facilitates other person’s illegal public transmission of copyright-protected works.

f) The sale of **Kodi boxes or similar devices.**

There is no explicit discussion about Kodi boxes in Japan. But, there is a court case, where the Supreme Court held that the distribution of a memory card that modifies game software constituted a tort as secondary liability under the Japanese Civil Code, on the ground that the distribution of the memory card incited users’ infringement of the right of integrity of the game software.⁶⁴⁶ Similarly, the sale of Kodi boxes can constitute a tort as a secondary liability under the Japanese Civil Code, according to the judgement.

g) Other types of unauthorized online use of copyright-protected content not listed above.

Nothing to report.

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

No.

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country’s law? If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.

⁶⁴⁴ Osaka District Court, 20 June 2013, 2218 Hanrei Jihō 112 [Rocket News 24 Case]. The translation is available at <http://www.ip.courts.go.jp/app/files/hanrei_en/893/000893.pdf>.

⁶⁴⁵ Tokyo District Court, 15 September 2016, Case No.17928 of 2015 [Retweet Case]; IP High Court, 25 April 2018, Case No.10101 of 2016 [Retweet Case, second instance]. Interestingly, the IP High Court held that the modification occurred by the “retweet” constituted the infringement of the right of integrity. The translation of the Tokyo District Court is available at <http://www.ip.courts.go.jp/app/files/hanrei_en/230/002230.pdf>.

⁶⁴⁶ Supreme Court, 13 February 2001, 55-1 Minshū 87 [Tokimeki Memorial Case]. The translation is available at <http://www.courts.go.jp/app/hanrei_en/detail?id=571>.

Under the ISP Liability Limitation Act (No.137 of 2001)⁶⁴⁷, ISPs (e.g. hosting providers) can benefit from liability exemption for damages, which applies not only to copyright infringement, but also to trade mark infringement and defamation.

Under the ISP Liability Limitation Act, even if any right of others is infringed by information distribution, an ISP shall not be liable for any loss incurred from such infringement unless (1) it is technically possible to take measures for preventing such information from being transmitted to the public, and (2a) in cases in which the ISP had known about the infringement of the rights of others by information distribution or (2b) in cases in which the ISP had had knowledge of information distribution itself and in which the ISP could reasonably know about the infringement of the rights of others (Act.3(2) of the ISP Liability Limitation Act).

Therefore, in case an ISP immediately acts upon the knowledge and removes the infringing content, it is not liable for damages under the ISP Liability Limitation Act.

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

With regard to video sharing platforms, a service provider of video sharing platforms can be regarded as a primary infringer, although it is basically regarded just an ISP.

In fact, there is a court case (TV Break Case) where the Court upheld the claim of not only damages but also injunction against a video-sharing platform, on the ground that the service provider was considered as the primary infringer in the normative sense by taking into account that the service provider had incited the user's uploading under its management in order to gain business profits and neglected the uploaded video files infringing copyrights without any measure to avoid that infringement.⁶⁴⁸

In case a service provider is not considered ISP but a primary infringer, it cannot benefit from safe-harbor or liability exemption, since the liability exemption does not apply where an ISP is considered the sender of the information that is deemed infringing under the ISP Liability Limitation Act (the second sentence of Art.3(1) of the ISP Liability Limitation Act).

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:

- The suspension from the internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.

⁶⁴⁷ The translation is available at <<http://www.japaneselawtranslation.go.jp/law/detail/?id=2088&vm=02&re=01&new=1>>.

⁶⁴⁸ IP High Court, 8 September 2010, 2115 Hanrei Jihō 102 [TV Break Case]. A translation is available at <<http://www.ip.courts.go.jp/hanrei/pdf/20111115132355.pdf>>.

- The monitoring or **filtering** of content.
- The **blocking** and removing of infringing content, including notice-and-takedown.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.
- Obligations imposed on service providers to notify public authorities of alleged infringing activities or information provided by recipients of their service.
- **Graduated response systems.**

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

Under the Japanese Copyright Act, copyright holders may demand an injunction against a primary infringer of copyright (Art.112(1)).

Under the Japanese Civil Code, copyright holder whose copyright has been infringed, either intentionally or negligently, may claim damages (Art.709).

b) Administrative.

In Japan, no administrative measure is provided as for copyright infringement.

c) Criminal.

Under the Japanese Copyright Act, the infringement of copyright is punishable by imprisonment with work obligation for up to 10 years or by a fine of up to JPY 10 million, or both (Art.119(1)).

In fact, according to news reports, a person who established the stream-ripping website named "Nico*Sound" that enables users to download music as MP3 file from the video sharing platform named "NicoNico Doga" was arrested for a crime of copyright infringement in 2014, because music works are recorded in his server and afterwards transmitted to users of the website without authorization of rightholders, which was considered a primary copyright infringement.

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law against intermediaries to address online copyright infringement by third party users of their services?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

Under the Japanese Copyright Act, there is no explicit provision (e.g. Art.8(3) of the Information Society Directive in the EU) or interpretation (e.g. the "Störerhaftung" in German law) which allows a copyright holder to demand an injunction against intermediaries.

With regard to damages, a person who incited or was an accessory to the infringement of the perpetrator shall be jointly and severally liable to compensate for damages, as a joint tortfeasor under the Japanese Civil Code (Art.719(2)).

As mentioned above (6), there is a court case (TV Break Case) where the Court upheld the claim of not only damages but also injunction against a video-sharing platform, on the ground that the service provider was considered as the primary infringer in the normative sense by taking into account that the service provider had incited the user's uploading under its management in order to gain business profits and neglected the uploaded video files infringing copyrights without any measure to avoid that infringement.⁶⁴⁹

On the other hand, under the ISP Liability Limitation Act, a person alleging that his/her rights have been infringed may demand that an ISP discloses the identification information of the sender pertaining to the infringement of the rights (e.g. name and address, IP Address, etc.) possessed by the ISP (Art.4(1)).

b) Administrative.

In Japan, no administrative measure is provided as for copyright infringement.

c) Criminal.

Under the Japanese Penal Code, a person who induces an accessory shall be dealt with in sentencing as an accessory (Art.62(2)).

There is a court case regarding a file sharing software named "Winny", where the Kyoto District court convicted the accused who released the software of a crime of inducing others' copyright infringement and the Osaka High Court as well as the Supreme Court however denied the crime on the ground that the accused lacked the intent of accessoryship to the crime of violation of the Copyright Act.⁶⁵⁰

9. To the best of your knowledge, are there significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

No.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

a) If yes, what conditions must be met for that obligation to arise?

Under the ISP Liability Limitation Act, a person alleging that his/her rights have been infringed may demand that an ISP discloses the identification information of the sender pertaining to the infringement of the rights (e.g. name and address, IP address, etc.) possessed by the ISP, provided that (1) there is evidence that his/her rights were infringed by the information distribution and (2) when the identification information of the sender is necessary in order for that person to exercise his rights

⁶⁴⁹ IP High Court, 8 September 2010, 2115 Hanrei Jihō 102 [TV Break Case]. A translation is available at <<http://www.ip.courts.go.jp/hanrei/pdf/20111115132355.pdf>>.

⁶⁵⁰ Supreme Court, December 19, 2011, 65-9 Keishū 1380 [Winny Case]. The translation is available at <http://www.courts.go.jp/app/hanrei_en/detail?id=1131>.

to claim damages, and where there is justifiable ground for him to receive disclosed identification information of the sender (Art.4(1) of the ISP Liability Limitation Act).

The ISP of whom the disclosure of identification information is demanded shall not be liable for any loss incurred by the person who demanded the disclosure arising from the ISP's refusal of the demand, unless there is any willful act or gross negligence on the part of the ISP (Art.4(4) of the ISP Liability Limitation Act).

There is also a precedent of the Supreme Court holding that an access provider (a cell-phone provider in the case at issue), who merely relays communications between a sender (primary infringer) and a hosting provider who manages and operates a server pertaining to an electronic bulletin board, falls under an ISP who shall be obliged to disclose the sender's identification information under Article 4(1) of the ISP Liability Limitation Act.⁶⁵¹

b) If yes, what type of personal data is typically requested?

For example, name, address or IP address of infringers.

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

Basically, copyright holders who have exclusive rights may demand injunction (Art.112(1) of the Japanese Copyright Act) and file a criminal complaint (Art.123(1)).

According to the major theories, not only copyright holders but also an exclusive licensee may demand injunction against infringers, at least in case the copyright holder is obliged to remove the infringing act.⁶⁵²

According to the major theories, not only copyright holders but also an exclusive licensee may demand damages against infringers, at least in case only the exclusive licensee exploits the work in the market.⁶⁵³

According to the Supreme Court, not only copyright holders but also an exclusive licensee may file a criminal complaint.⁶⁵⁴

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

- Please indicate whether the measures refer to public or private enforcement.

There are a lot of court cases in Japan where copyright holders demand a disclosure of the identification information of infringers against ISPs under the ISP Liability Limitation Act, as public enforcement.

a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?

⁶⁵¹ Supreme Court, 8 April 2010, 64-3 Minshū 676 [Relay Provider Case]. The translation is available at <<http://www.courts.go.jp/english/judgments/text/2010.04.08-2009.-Ju-.No..1049.html>>.

⁶⁵² See Tokyo District Court, January 31, 2002, 1818 Hanrei Jihō 165 [Tonttu doll Case]; Tokyo District Court, September 28, 2016, Case No.482 (wa) of 2015 [Smartphone cover Case].

⁶⁵³ See Tokyo District Court, April 15, 2015, Case No.24391 (wa) of 2014 [Amana images Case].

⁶⁵⁴ See Supreme Court, April 4, 1995, 49(4) Keishū 563, [Pirate video Case].

Nothing special.

- b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.**

Nothing special.

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

It is now under discussion in Japan, whether to introduce a new provision to deem a website that knowingly aggregate a lot of hyperlinks to illegal/unauthorized copyright-protected contents (often called a “leech site”) as a primary copyright infringement.

The Intellectual Property Strategic Program 2016 (May 9, 2016) of the Japanese Government proposed to consider an appropriate response to the problem.⁶⁵⁵ Also, the Intellectual Property Strategic Program 2017 (May 16, 2017) of the Japanese Government proposed to continue to consider the issue.

Against this background, the issue is now discussed in the Sub-committee on Legal and Fundamental Issues of the Subdivision on Copyright of the Council for Cultural Affairs of Japan, as one of the main agendas since 2017.

A site-blocking order is not allowed in Japan now. But, the Intellectual Property Strategic Program 2016 (May 9, 2016) of the Japanese Government proposed to “engage in ongoing discussion which includes the effects and impacts of website blocking efforts in other countries aimed at online IP infringement”.⁶⁵⁶ Also, the Intellectual Property Strategic Program 2017 (May 16, 2017) of the Japanese Government proposed to continue to consider the issue.

The Intellectual Property Policy Headquarters published the emergency plan against copyright infringing websites on 13 April 2018, which encouraged ISPs to conduct a site-blocking under certain conditions and announced the establishment of a legal system for enabling a site-blocking by ISPs. Against this background, the task-force meeting for this issue is to be established in June 2018.

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions/campaigns aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

Generally speaking, some institutions including the Japanese Society for Rights of Authors, Composers and Publishers (JASRAC) for music, the Japan and International Motion Picture Association (JIMCA) for movies, the Association of Copyright for Computer Software (ACCS) for computer software and the Content Overseas Distribution Association (CODA) are engaged in non-legal actions or campaigns on online infringement.

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

⁶⁵⁵ The translation is available at <http://www.kantei.go.jp/jp/singi/titeki2/kettei/chizaikaku20160509_e.pdf>.

⁶⁵⁶ See *supra* note 655 at 16.

Under the Japanese Copyright Act, there is no explicit provision which allows a copyright holder to demand an injunction against intermediaries, while an injunction against a primary infringer is permitted under Article 112 of the Japanese Copyright Act.

Therefore, case law has held several online platforms liable for copyright infringement by expanding the substantive scope of a primary “infringer” based on the normative interpretations including the so-called “Karaoke theory”; an online video sharing platform,⁶⁵⁷ a P2P file sharing service⁶⁵⁸ and an online electronic bulletin board,⁶⁵⁹ while the Karaoke theory has been criticized by academics on the ground that it unreasonably expands the scope of a primary “infringer” without a clear dogmatic basis or theoretical rationale.⁶⁶⁰

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

No.

⁶⁵⁷ IP High Court, 8 September 2010, 2115 Hanreijihō 102 [TV Break Case].

⁶⁵⁸ Tokyo High Court, 31 March 2005, Case No.405 (ne) of 2004 [File Rogue Case].

⁶⁵⁹ Tokyo High Court, 3 March 2005, 1893 Hanrei Jihō 126 [2-Channel Case].

⁶⁶⁰ See Tatsuhiro Ueno, Intellectual Property Liability of Consumers, Facilitators and Intermediaries: The Position in Japan, in: Christopher Heath / Anselm Kamperman Sanders (ed.) Intellectual Property Liability of Consumers, Facilitators and Intermediaries (Kluwer 2012), p.143.

Questionnaire Thailand

NING (NONTAYA) CHULAJATA and FABRICE MATTEI, Rouse Thailand

Last updated: 11 June 2018

Section 1: Online Copyright Infringement and Enforcement in National Law

The following questions all relate both to statute law and case law (jointly referred herein as ‘national law’). Please add the sources to your reply (legislative provision, leading cases, etc.).

This section aims at understanding how your national law regulates online copyright infringement and enforcement. In this section, the term ‘copyright’ includes also related or neighboring rights. The questions are divided into two subsections. The first addresses the relevant legal rules on online copyright infringement in your national law. The second refers to national enforcement measures, procedures, remedies and sanctions. Technical terms defined in the glossary in Annex are color coded red.

Legal Rules on Online Copyright Infringement

1. What legal instruments regulate online copyright infringement in your national law? Please provide a list of the instruments.

- Copyright Act B.E. 2537 (1994) (as amended by the Copyright Acts (No.2 and 3) B.E. 2558 (2015)) (“the Copyright Act”)
- Computer-Related Crime Act B.E. 2550 (2007) (as amended by the Computer-Related Crime Act (No.2) B.E. 2560 (2017)) (“the Computer-Related Crime Act”)
- Penal Code (Chapter 6: Principals and Supporters)
- Civil and Commercial Code (Title 5: Wrongful Acts)

2. How does your national law approach the notion of ‘intermediary’ in the context of copyright? Are there relevant provisions that define the notion or specific types of intermediaries (e.g. ISPs, hosting providers, etc.)?

The notion of ‘intermediary’ under Thailand’s national law is defined as ‘service provider’. Under section 32/3 of the Copyright Act and section 3 of the Computer-Related Crime Act, the meanings of ‘Service Provider’ are similarly provided as follows:

- A Service Provider to others in accessing the internet or enabling others to contact one another by other means through a computer system whether the Service Provider does so under his name, or those of others or in the interests of others.
- Service Provider for computer information storage for the interest of others.

3. Does your national law qualify the following acts as copyright infringement?

This question contains a list of acts that may qualify as copyright infringement. In answering the question for each act, please explain whether their legal qualification:

- Depends on knowledge or awareness by the user of the illegal/unauthorized status or source of the

protected content;

- Depends on the commercial or for-profit nature or intent of the use or user;
- Is uncertain and, if so, why;
- Varies depending on the type of protected content (music, audio-visual, books, and video games). If that is the case, please cite and/or describe as completely as possible the relevant differences.

a) Downloading copyright-protected content from illegal/unauthorized sources on the Internet.

The meaning of ‘Reproduction’, means any method of copying, imitation, duplication, blockmaking (i.e. mold making), sound recording, video recording or sound and video recording for the material part from the original, copy or publication whether of the whole or in part⁶⁶¹.

Thus, downloading is the reproduction which is one of exclusive rights of the copyright’s owner⁶⁶². An act of downloading copyright-protected content from illegal/unauthorized sources on the Internet is a copyright infringement⁶⁶³.

The act of reproduction from an illegal/unauthorized source would not benefit from “personal use” exception as it does not fall within the exception’s conditions i.e. the personal use 1) does not conflict with the copyright owner’s normal exploitation and 2) does not reasonably prejudice the legitimate right of the copyright owner. Thus, yes, the exception applies only to copies made from legal/authorized sources on the Internet.

The specific legal provision varies for the following types of protected content:

- The downloading of audio-visual is a copyright infringement under Section 28 of the Copyright Act.
- The downloading of video game is a copyright infringement under Section 30 of the Copyright Act as the video game is ‘computer program’ (instructions, set of instructions or anything which are used with a computer so as to make the computer work or to generate a result no matter what the computer language is)⁶⁶⁴.

As for the remaining types of protected content i.e. music⁶⁶⁵ and books, they would be covered by the general copyright infringement under Section 27 of the Copyright Act. Please note that the copyright infringement of “sound recording” will be governed by Section 28⁶⁶⁶.

b) Streaming copyright-protected content from illegal/unauthorized sources on the Internet.

The streaming is deemed to be under the definition of ‘Communication to public’, i.e. making the work available to public by means of performing, lecturing, preaching, playing music, causing the

⁶⁶¹ Copyright Act B.E 2537 (1994) (as amended by the Copyright Acts (No.2 and 3) B.E. 2558 (2015) (Copyright Act), Sec. 4.

⁶⁶² Ibid, Sec. 15.

⁶⁶³ Ibid, Sec. 27.

⁶⁶⁴ Ibid, Sec. 4.

⁶⁶⁵ Under Sec. 4 of the Copyright Act, “musical work” means a work with respect to a song which is composed for playing or singing whether with rhythm and lyrics or only rhythm, including arranged and transcribed musical note or musical diagram.

⁶⁶⁶ Under Sec. 4 of the Copyright Act, “sound recording” means a work which consists of sequence of music, sound of a performance or any other sound recorded on any kind of material and capable of being replayed with an equipment necessary for such material but not including the sound track of a cinematographic work or another audiovisual work.

perception by sound or image, constructing, distributing or by any other means⁶⁶⁷, which is exclusive right of the copyright's owner⁶⁶⁸.

Thus, streaming copyright-protected content from illegal/unauthorized sources on the Internet is a copyright infringement⁶⁶⁹.

The specific legal provision varies for the following types of protected content:

- The streaming of audio-visual is a copyright infringement under Section 28 of the Copyright Act.
- The streaming of video game is a copyright infringement under Section 30 of the Copyright Act as the video game is 'computer program' (instructions, set of instructions or anything which are used with a computer so as to make the computer work or to generate a result no matter what the computer language is)⁶⁷⁰.

Although we are not aware of precedents on this issue, we take the view that reception of streaming may constitute a copyright infringement as it may be considered a reproduction.

The new Section 32/2 of the Copyright Act provides an exception for unavoidable temporary copying by/through computer system—specifically “Acts conducted to a work enjoying copyright lawfully created by or acquired through a computer system which are in the form of reproduction necessary for the use of a copy of the work in order to enable the equipment used in the computer system or the process for transmission or a work enjoying copyright via the computer system to work properly shall not be deemed copyright infringement”. However, we believe that this Section is intended to only capture reproduction that is necessary for the system to operate normally, and it is unlikely to cover streaming. Since it may not fall into the exception, the reception of streaming may amount to copyright infringement.

c) Stream-ripping copyright-protected content.

The stream-ripping, equivalent to downloading, of copyright-protected content from illegal/unauthorized sources on the Internet is a copyright infringement⁶⁷¹ against the exclusive right of the copyright's owner⁶⁷². The answers in a) therefore apply. Stream-ripping under Thai laws is not specifically mentioned. But certain types of stream ripping may be considered circumvention of technological measures and thus infringement of technological measures under Section 53/4 of the Copyright Act.

d) Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder.

The uploading is deemed to be under the definition of 'Communication to public'⁶⁷³. Thus, the act of uploading copyright-protected content without authorization is a copyright infringement⁶⁷⁴ against the exclusive right of the copyright's owner⁶⁷⁵.

The specific legal provision varies for the following types of protected content:

- The uploading of audio-visual is a copyright infringement under Section 28 of the Copyright Act.

⁶⁶⁷ Ibid.

⁶⁶⁸ Copyright Act, Sec. 15.

⁶⁶⁹ Copyright Act, Sec. 27.

⁶⁷⁰ Copyright Act, Sec. 4.

⁶⁷¹ Copyright Act, Sec. 27.

⁶⁷² Copyright Act, Sec. 15.

⁶⁷³ Copyright Act, Sec. 4.

⁶⁷⁴ Copyright Act, Sec. 27.

⁶⁷⁵ Copyright Act, Sec. 15.

- The uploading of video game is a copyright infringement under Section 30 of the Copyright Act.
- e) **Posting hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder.**
 - *Please specify if the answer varies depending on the type of hyperlinking technique in question (e.g. standard surface hyperlink, deep-link, embedded or framing hyperlink).*

The posting of hyperlinks to copyright-protected content is deemed to be under the definition of ‘Communication to public’⁶⁷⁶. Thus, the act of posting of such hyperlinks without expressing authorization of the right holder is a copyright infringement⁶⁷⁷ against the exclusive right of the copyright’s owner⁶⁷⁸. In Thailand, unfortunately, we are unaware of any published case involving the legal qualification of hyperlink.

The answer would be the same with vary types of hyperlinking technique.

f) The sale of Kodi boxes or similar devices.

The sale of Kodi boxes or similar devices, for profit, is a copyright infringement in case the sellers know or should have known that the copyright-protected work has been obtained by copyright infringement.⁶⁷⁹ The copyright infringement in question is the infringement to the copyright owner’s exclusive rights of making available to the public. It is noted that the knowledge of the illegal/unauthorized status is a condition of copyright infringement for this activity and the sales must be for profit.

g) Other types of unauthorized online use of copyright-protected content not listed above.

The unauthorized online use of copyright-protected content that shall be considered copyright infringement, apart from reproduction and communication to public, only for audio-visual and video-game, is letting (i.e. rental) the original or copy of the copyrighted work according to the Copyright Act section 28 and section 30 respectively.

The definition of letting/rental is a contract whereby a person – the letter – agrees to let another person – the hirer – have the use or benefit of a property for a limited period of time and the hirer agrees to pay rent therefore⁶⁸⁰, and therefore covers rental by any means including online.

The types of content that online rental is prohibited is audiovisual work, cinematographic work, sound recording and computer program, according to Section 28 and 30 of the Copyright Act.

However, if the rental is for profit, it will cover any content that known or should have been known that it is made by infringing the copyright of another person, according to Section 31 of the Copyright Act.

Section 31 of the Copyright Act addresses secondary liability where an infringer obtains the copyrighted infringing work (knowing or should have known that the work is made by copyright infringement) and let of the work. While, Section 28 and 30 are cases of direct infringement (liability) that the infringers have accessed to the original work and letting of the original or copies of the work. Thus, the difference is not whether the rental is for profit or not, but whether the infringer is the direct or secondary one.

⁶⁷⁶ Copyright Act, Sec. 4.

⁶⁷⁷ Copyright Act, Sec. 27.

⁶⁷⁸ Copyright Act, Sec. 15.

⁶⁷⁹ Copyright Act Sec. 31.

⁶⁸⁰ Civil and Commercial Code Sec. 537.

According to the activities above listed, except from the selling of Kodi boxes, knowledge or awareness by the user of the illegal/unauthorized status or source of the protected content is required for criminal punishment⁶⁸¹. For the sale of Kodi boxes, infringement arises if infringer knows or just should have known of the illegal/unauthorized status.

The acts of copyright infringement that do not conflict with a normal exploitation of the copyright work by the owner of copyright and do not reasonably prejudice the legitimate right of the owner of copyright shall not be deemed an infringement of copyright if it is a research or study of the work which is not for profit, or use for personal benefit (i.e. personal use) or falls within other exemptions provided in section 32 and, for computer program, section 35 of the Copyright Act.

Thus, as mentioned above, the act of reproduction from an illegal/unauthorized source would not benefit from the exception.

The full English translation of the amended Copyright Act is not available. Please find below the links for the Copyright Act B.E. 2537 (1994) (before amendment) and the Copyright Acts (No. 2 and 3) B.E 2558 (2015):

- <http://www.wipo.int/edocs/lexdocs/laws/en/th/th001en.pdf>
- [http://web.krisdika.go.th/data/outsitedata/outside21/file/COPYRIGHTACT \(NO.2\), B.E. 2558 \(2015\).pdf](http://web.krisdika.go.th/data/outsitedata/outside21/file/COPYRIGHTACT (NO.2), B.E. 2558 (2015).pdf)
- [http://web.krisdika.go.th/data/outsitedata/outside21/file/COPYRIGHTACT \(NO.3\), B.E. 2558 \(2015\).pdf](http://web.krisdika.go.th/data/outsitedata/outside21/file/COPYRIGHTACT (NO.3), B.E. 2558 (2015).pdf)

4. Does your national law differentiate between acts of copyright infringement by minors and by adults and, if so, what are the relevant differences?

Under the Copyright Act, there is no difference between the infringement conducted by minors and by adults. However, under section 73-76 of the Penal Code, the criminal punishment would be different for a person under the age of twenty (i.e. minors⁶⁸²).

Section 73-76 of the Penal Code provides exemption and options on punishment to minors. That is, 1) the infringer not over 10 years old shall not be punished (Section 73), 2) the infringer over 10 years old but not over 15 years old shall not be punished but the court may have any additional injunction listed in Section 74, 3) the infringer over 15 years old but lower than 18 years old, upon the court discretion, might not be punished as provided in Section 74 or be punished with a reduce scale of punishment provided for the offence by half (Section 75), and 4) the infringer having an age of 18 years old but not over 20 years old might be punished with a reduce scale of punishment provided for the offence by one-third or half (Section 76).

5. Do online intermediaries benefit from liability exemptions or safe-harbors in your country's law? If yes, please cite and/or describe as completely the scope of the exemptions or safe-harbors.

The intermediaries' liability exemptions are provided under section 32/3 of the Copyright Act. That is, if the intermediaries - i.e. Service Provider under the act - does not control, initiate or command the infringement of the copyrighted material in their computer system and such Service Provider complies with the Court order against the infringing content, they will not be liable for acts relating to the infringement of copyright that occurred prior to the Court order and after the court order is no longer effective. The liability exemption in S32/3 applies explicitly to damages. The provision is silent on other measures, so we believe that the exemption should be limited damages only.

⁶⁸¹ Penal Code Sec. 59.

⁶⁸² Civil and Commercial Code Sec. 19.

6. Is there uncertainty in your national law as to whether certain activities of online intermediaries give rise to primary liability or benefit from safe-harbors? If yes, please cite and/or describe as completely as possible the relevant differences?

The criteria for safe-harbors are the Service Provider must 1) not control, initiate or command the infringement of the copyrighted material in their computer system, and 2) complies with the Court order against the infringing content.

However, according to section 20 of the Computer-Related Crime Act as provided in Section 14 of the Computer Crimes Act (No.2) (available at [https://en.wikisource.org/wiki/Translation:Computer_Crimes_Act_\(No._2\)_2017](https://en.wikisource.org/wiki/Translation:Computer_Crimes_Act_(No._2)_2017)), the Court by a petition of competent officer with approval of the Minister could order for suppression of dissemination or removal of computer data which is a copyright infringement from a computer system. But, no safe-harbor for Service Provider is provided in this case. The provision allows the authority to both suppress the dissemination of copyright work and delete the infringing data.

Thus, there is uncertainty for the Service Provider receiving court's order under section 20 of the Computer-Related Crime Act whether they could enjoy the liability exemption or not.

The Computer Related Crime Act only applies to copyright infringement that qualifies as a crime.

Regarding Section 32/3 of the Copyright Act, in the last paragraph, it is not clearly specific that the safe harbors is for damages from copyright infringement under Civil Law only. But, it shall cover any damage (whether monetary or not) that the Service Provider might be claimed arising from implementing the Court's order.

As mentioned above that safe harbor is not provided under the Computer Related Crime Act, in case the intermediaries are ordered to remove the data under Section 20 of the Computer Related Crime Act, they cannot avoid paying damages if claimed. Safe harbor would be available when the copyright owner chooses to file a petition to Court under Section 32/3 of the Copyright Act and the Service Provider (intermediaries) follow the Court's order as such.

Enforcement measures, procedures, remedies, and sanctions

This subsection aims to describe the set of public and private enforcement measures, procedures, remedies, and sanctions against online copyright infringement available in national law. These measures can be civil (e.g. injunctions), administrative (e.g. warnings), or criminal (e.g. prison sentences).

Enforcement measures may be aimed at the direct infringer (the user of protected content) or at intermediaries. In the latter case, the aim of the measures is for the intermediaries to end or prevent infringement by third party users of their services. Examples of measures that may be taken by intermediaries to prevent or end infringement are:

- The suspension from the internet of the infringer, e.g. through the termination of the subscription or client account of the user.
- Measures for identification of the infringer, e.g. through injunctions that order that identification.
- The monitoring or filtering of content.
- The blocking and removing of infringing content, including notice-and-takedown.
- Warning systems, such as posting notices to users on the illegality of copyright infringement and that the intermediary's services cannot be used for its commission.
- Obligations imposed on service providers to notify public authorities of alleged infringing

- activities or information provided by recipients of their service.
- Graduated response systems.

7. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law to address online copyright infringement by users (whether individuals or websites/platforms)?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil

The specific civil measure designed for online copyright infringement is not available. The law provides generally on civil lawsuit against users conducting copyright infringement, claiming for damages and injunctions, is available under the wrongful acts of the Civil and Commercial Code.

b) Administrative.

Under section 20 of the Computer-Related Crime Act, the administrative enforcement is available as the Court by a petition of competent officer with approval of the Minister could order for suppression of dissemination or removal of computer which is a copyright infringement from a computer system.

In case the users fail to comply with the court order, they will be subject to a fine not exceeding 200 thousand Baht and a further daily fine not exceeding 5 thousand Baht per day until the relevant corrective action has been taken.⁶⁸³

Section 20 of the Computer-Related Crime Act applies to any copyright infringement that constitute a crime. But, in case the copyright infringement bears characteristics which are contrary to peace and order or good morals, the procedure under Section 20 paragraph two (not 20/3 as you mentioned) will be applied. That is, the approval of a computer data screening panel is required for the Minister to authorize a competent authority to file an application to Court.

c) Criminal.

The copyright's owner could file a criminal lawsuit against the users conducting copyright infringement. But, as the offences under the Copyright Act is compoundable offences⁶⁸⁴, the damaged person must lodge a complaint within three months as from the date of offence and offender to be known. Otherwise, the prosecution is barred by prescription. In any case, the criminal lawsuit could be filed individually by the injured person or through the public prosecutor.

Regarding the criminal offences relating to online copyright of activities listed above, the offences are under section 69 of the Copyright Act. That is, offence against protected music, audio-visual, books, and video games is punishable by a fine from 20 thousand Baht up to 200 thousand Baht (approx. from USD 600 to USD 5,990). In case the offence is committed with the commercial purpose, the offender shall be inflicted with imprisonment for a term from six months up to four years or a fine from 100 thousand Baht up to 800 thousand Baht (approx. from USD 2,994 to USD 23,952) or both imprisonment and fine.

But, for the selling of Kodi boxes or similar devices for profit that the sellers know or should have known that the copyright-protected work has been obtained by copyright infringement, the offence is

⁶⁸³ Computer-Related Crime Act Sec. 27.

⁶⁸⁴ Copyright Act Sec. 66.

under section 70 of the Copyright Act, which is by a fine from 10 thousand Baht up to 100 thousand Baht (approx. from USD 300 to USD 2,994). If the offence is committed with the commercial purpose, the offender shall be inflicted with imprisonment for a term from three months up to two years or a fine from 50 thousand Baht up to 400 thousand Baht (approx. from USD 1,497 to USD 11,975) or both imprisonment and fine.

8. What civil, administrative, and criminal enforcement measures, procedures, remedies, and sanctions are available under your country's law against intermediaries to address online copyright infringement by third party users of their services?

- When answering this question, please note any differences that may apply depending on the type of protected content (music, audio-visual, books, and video games).

a) Civil.

Civil lawsuit against intermediaries could be enforceable in case it is proved that the intermediaries are negligent causing damages to the copyright's owner, under the wrongful acts of the Civil and Commercial Code. Copyright owner may ask for damages and injunctions.

b) Administrative.

The administrative measures mean those available through actions of government officers without filing of lawsuit required.

The court order to Service Provider for refrain or removal of the claimed copyright infringement from the Service Provider's computer system is available under section 32/3 of the Copyright Act and for suppression of dissemination or removal of computer which is a copyright infringement from a computer system under section 20 of the Computer-Related Crime Act.

Section 32/3 of the Copyright Act is classified as administrative enforcement because it is not the case where the copyright owner files a lawsuit against the Service Provider and requests for injunction. It is an administrative procedure that the copyright owner could solely submit a request for Court's order. The competent court in this case is the Central Intellectual Property and International Trade Court.

Under the Copyright Act, there is no penalty for the Service Provider not following the court's order. But, for the same case under the Computer-Related Crime Act, a fine not exceeding 200 thousand Baht and a further daily fine not exceeding 5 thousand Baht per day until the relevant corrective action has been taken is prosecuted⁶⁸⁵.

Apart from the fine, if the intermediary does not follow the court order, a civil lawsuit against the intermediary as mentioned above is possible. Please note that the civil lawsuit mentioned here means an option of filing a civil lawsuit is still available.

c) Criminal.

No criminal enforcement for intermediaries not knowing of the copyright infringement is provided.

9. To the best of your knowledge, are there significant differences in public and private enforcement practices depending on the type of protected content (music, audio-visual, books, and video games)? If yes, please cite and/or describe as completely as possible the relevant differences.

⁶⁸⁵ Computer-Related Crime Act Sec. 27.

There is no difference in public and private enforcement practices relating to different types of protected content.

10. Do online intermediaries have an obligation to disclose personal data of individuals involved in copyright infringing activities to rights holders?

- a) If yes, what conditions must be met for that obligation to arise?
- b) If yes, what type of personal data is typically requested?

There is no obligation for intermediaries to disclose personal data of the user unless the disclosure is under the court's order or subpoenas⁶⁸⁶.

11. Who can apply for the copyright enforcement measures, procedures, remedies, and sanctions under national law?

- Civil enforcement

Copyright's owner or authorized persons

Authorized person includes any person that their rights have been disputed, according to Section 55 of the Civil Procedure Code. Thus, it covers licensees and collecting societies where their rights relating to copyright are disputed, provided they have evidentiary documents to prove their authorization from the copyright's owner.

- Administrative enforcement

For the court's order to Service Provider for refrain or removal of the claimed copyright infringement from the computer system under the Copyright Act, the Copyright's owner or authorized persons could apply for the enforcement.

For the court's order for suppression of dissemination or removal of computer which is a copyright infringement from a computer system under section 20 of the Computer-Related Crime Act, the competent officer (could be from a request of copyright's owner) with approval from the Ministry could apply for the enforcement.

- Criminal enforcement

The enforcement could be initiated by the damaged person or the public prosecutor⁶⁸⁷.

12. To the best of your knowledge, what are the most widely used and/or effective enforcement measures, procedures, remedies, and sanctions against infringing users and intermediaries in your country?

- Please indicate whether the measures refer to public or private enforcement.⁶⁸⁸

⁶⁸⁶ Constitution of Thailand Sec. 36.

⁶⁸⁷ Penal Code Sec. 28.

⁶⁸⁸ In this context, 'public enforcement' refers to the use of public agents, agencies, bodies or authorities to detect and to sanction copyright infringers, whereas 'private enforcement' refers to the threat of litigation by private parties, namely rights holders or their representatives.

Regarding the enforcement against users, the enforcement most widely used or common practice for enforcement would be criminal enforcement through police authorities, as it is more convenient and cost effective. However, a direct warning for removal of infringing content is normally used in private enforcement prior to the criminal enforcement as well.

Options for enforcement against intermediaries under both the Copyright Act and Computer-Related Crime Act have only recently come into force, actual enforcement against intermediaries may have not likely occurred.

a) Was any of these measures introduced in your national law or did it become more relevant in the practice of enforcement over the last three years?

Yes, the enforcement options against intermediaries just become available in 2015 and early 2017.

b) If available, please provide one or two examples of the application of these measures in high profile cases in your country over the last three years.

One example was the closing of the website kodhit.com which is a popular website in Thailand for downloading Korean movies and series with Thai subtitles, because it appears to have received a takedown notice⁶⁸⁹.

13. To the best of your knowledge, what are the main topics of debate in your country regarding private or public enforcement against online copyright infringement over the last three years? Please provide a short summary.

Recently, most of the debate relating to enforcement against online copyright infringement are enforcement for taking down the copyright infringing content. Since the modification of the Copyright Act in 2015, followed by the modification of the Computer-Related Crime Act in 2017, the concerns are on whether the amended provisions are effective in practice. For example, what are sanctions for the Service Provider not following the court's order under the Copyright Act and whether the court's order is enforceable against the user/Service Provider not having the domicile in Thailand. In addition, for the Copyright Act, the provision imposes only injunction against intermediary⁶⁹⁰.

14. Do you know of any non-legal actions/campaigns on online copyright infringement, such as awareness, education and information campaigns, taking place in your country over the last three years? If yes, were these actions/campaigns aimed at specific illegal/unauthorized channels? Who initiated and sponsored these actions/campaigns?

Examples of campaign on online copyright infringement are “Downloading for fun does matter” by TrueVisions, the leading cable and satellite television operator in Thailand⁶⁹¹. The campaign is

⁶⁸⁹ “พาณิชย์” ย้ำเว็บโคตรฮิตทำซ้ำไทยซีรีส์เกาหลี ผิดกม.ลิขสิทธิ์ ฐานทำซ้ำและเผยแพร่ มีโทษทั้งปรับทั้งจำ' MRG Online (17 November 2016) <<http://www.manager.co.th/iBizChannel/ViewNews.aspx?NewsID=9590000115106>> accessed 24 July 2017.

⁶⁹⁰ Sinfah Tunsarawuth, ‘Thailand Toughens Copyright Law To Deal With Internet Providers, Unlawful Movie Recording In Theaters’ (Intellectual Property Watch, 1 April 2015) <<https://www.ip-watch.org/2015/04/01/thailand-toughens-copyright-law-to-deal-with-internet-providers-unlawful-movie-recording-in-theaters/>> accessed 24 July 2017; ‘รัฐรู้ยัง! เว็บละเมิดมี “หนังโป๊-พนัน” เป็นสปอนเซอร์ใหญ่ สมาคมหนังสหรัฐฯ จี้ไทยแก้ไขด่วน’ MGR Online (20 March 2016) <<http://www.manager.co.th/iBizChannel/ViewNews.aspx?NewsID=9590000028921>> accessed 24 July 2017.

⁶⁹¹ ‘ทรูวิชั่นส์ ร่วมสนับสนุน โครงการรณรงค์ออนไลน์ต่อต้านการละเมิดลิขสิทธิ์’ CP e-NEWS (7 April 2014) <<http://www.cpthailand.com/รวมคอลมน/tabid/129/articleType/ArticleView/articleId/2509/-.aspx>> accessed 24 July 2017.

cooperated with the US Embassy of Thailand and aimed for raising awareness in online copyright infringement and educate options for legal use of copyrighted content online. No specific illegal/unauthorized channel is mentioned.

15. Are there any other issues relevant for online copyright enforcement that are specific to your country but not addressed in this questionnaire?

The issue of whether measures provided by related laws is effective in practice should be mentioned. That is, although the amended Copyright Act and Computer Crime Act seem to benefit the copyrights' owner by providing tools for take down of copyright infringing content, there are concerns that it might not be as effective as it should be. The examples of debates concern Court' criteria to issue the order under the two acts which are not specifically provided and limitations of court' orders for Service Provider hosted outside Thailand.

16. Do you have any suggestions on national-level studies and/or data on enforcement statistics regarding online copyright infringement?

N/A

ANNEX 3: Summary Tables Question 3 – online acts qualified as copyright infringement

[Tables start on the following page]

Color code for tables



Yes

Probably Yes / More Likely than Not

No

(legal) uncertainty

Not Discussed on Not Applicable
(N/A)

Additional explanations through text
may be required in some cases.
These are inserted in the applicable
cell.

Exception	Applicable exception: private use/copy?								YES, but 2 regimes: general PC exception (S.29.22), Specific regime for musical sound recordings (S.79 et seq)	YES, possible fair dealing defence (for the purpose of research, private study, criticism, review, news reporting, education + reqs of acknowledgment and removal)	YES, general exception / fair dealings clause for non-commercial use (s. 46 © Act). '		
	Applicable if: authorised source?	YES but: obviously illegal source							YES general PC exceptions; NO explicit requirement of source for musical sound recordings exception			Unclear from response but presumed	
	Applicable if: non-commercial use?						✓		Deduced from other conditions for both exceptions	see above fair dealing		Unclear from response but presumed	Unclear from response but presumed
	Applicable if: knowledge or intent?									N/A			
	Exception remunerated?								NO for general private copying exception (S. 29.22); YES for musical sound recordings (S.79 et seq)			not discussed	not discussed
	Differences per content type relevant to study?	NO (but: VG as SW not discussed)	NO (but: VG as SW not discussed)	✓ Exception not applicable to video games (=software)	Exception not applicable to video games (=software)	NO (but: VG as SW not discussed)	Exception not applicable to entire books and (probably) VGs (=SW)		YES, 2 regimes: general PC exception (S.29.22), Specific regime for musical sound recordings (S.79 et seq)			Not discussed, but see content type differences exclusive right	
	Legal uncertainty application exception?				see supra				No explicit mention of requirement of source for S.81 may create uncertainty	case by case	case by case		
	Downloading from illegal/unauthorised source infringing copyright (civil)?				Yes for video games, but unclear for other content			Probable but uncertain	YES, except for musical sound recordings (apparently non-infringing)	Possible Fair Dealing	YES, if for commercial purposes. No, if non-commercial	YES (for digital sound or visual recordings)	

Question 3b: Streaming copyright-protected content from illegal/unauthorized sources on the Internet

Question 3b: Streaming copyright-protected content from illegal/unauthorized sources on the Internet

		Europe						Americas		Asia				
		France FRA	Germany DEU	Netherlands NLD	Poland POL	Spain ESP	Sweden SWE	United Kingdom GBR	Brazil BRA	Canada CAN	Hong Kong HKG	Indonesia IDN	Japan JAP	Thailand THA
Exclusive Right	Active Streaming (emission) is restricted act? under C2P right?		not discussed	not discussed	not discussed		not discussed						not discussed	
			id	id	id		id		distribution right + broadcasters' signal rights + possibly transmission rights		Probably NO	Performance Right	not discussed	
	Other exclusive righth(s)?		id	id	id		id						not discussed	
	under general exploitation clause?		id	id	id		id						not discussed	
	Passive Streaming (reception) is restricted act?	NO in general, but YES if through unauthorized kodi box	at least through unauthorized kodi box							Probably NO (but no case law yet)	Probably NO		Probably NO, but possibility that it can qualify as a transient reproduction in part	Probably YES
	Under reproduction right?												Probably NO, but possibility that it can qualify as a transient reproduction in part	
	under general exploitation clause?													
	restricted only if knowledge/awareness of illegal/unauthorised source							Uncertain for active streaming						
	restricted only if commercial or for-profit?													
	Differences per content type?	NO (presumed; not discussed)			NO (presumed; not discussed)		NO (presumed; not discussed)		NO (presumed; not discussed)					
	Legal uncertainty application of right?	SOME, to the extent it derives from recent CJEU case law	NO (REP right applies to permanent + temporary copies)	SOME, namely whether Filmspeier applies only in the scenario of unauthorized kodi boxes or to all types of passive streaming								Probably NO, but possibility that it can qualify as a transient reproduction in part	YES for passive streaming, as there are no legal precedents	

Exception	Applicable exception: temporary / transient use?	NO, if streaming via unauthorized kodi box	2 Exceptions potentially applicable: Private use/copying (s.53) + Temp/Transient (s.44a)	NO, if streaming via unauthorized kodi box	Possible application of Private use exception (= downloading) // Temp transient not discussed	NO (fails to meet reqs of: lawful use + lack of independent economic significance) Probably NO after CJEU Filmspelers (before it was considered that the exception applied, as it did not require legality of the copy)			IF one considers passive streaming reproduction, THEN essential temp/trans Exception in s.30,71 applies (Intermediaries protected by hosting safe harbor)		Exception only for 'news' regarding active streaming.	IF passive streaming = transient REP in part, THEN Exception for Reproduction required for the exploitation of works on computer applies (47 octies)	Probably NO: Exception exists for "unavoidable temporary copying..." (s.32.2) but probably not applicable
	Applicable if: authorised source?	YES for the unauthorized kodi box scenario (other types of streaming do no qualify as infringement, even if from unauthorized sources)	YES for Private use/copying (s.53), = downloading; UNCLEAR for Temp/Transient (CJEU Filmspelers might mean that lawful source is required)	YES for the unauthorized kodi box scenario		Probably YES after CJEU Filmspelers	Probably YES after CJEU Filmspelers (but there was already UK case law before not applying this defence to passive streaming)	✓	Possible uncertainty on the "facilitate a non-infringing use" language in s.30.71, which likely does not rule out its application to end-users				
	Applicable if: non-commercial use?		YES for Private use/copying (s.53)										
	Applicable if: knowledge or intent?			YES: knowledge of unauthorized source = indication that streaming not for lawful use									
	Exception remunerated?												
	Differences per content type relevant to study?				Exception not applicable to video games (=software)								
	Legal uncertainty application exception?	same as for the exclusive right above	NO for PC but UNCERTAINTY for Temp/Transient exception		see supra		see supra						YES, see above. Lack of precedents and uncertain application of exception
Streaming from illegal/unauthorised source infringing copyright (civil)?		If through unauthorized kodi box	Probably, but uncertain application of Temp/Transient exception	YES, at least through unauthorized kodi box (uncertain application to other passive streaming scenarios)		Probably YES after CJEU Filmspelers, but no case law yet and prior situation exempted these uses under Temp/Transient exception		Yes for Active Streaming and Uncertain / unlikely for Passive Streaming	YES for Active Streaming and Probably NO for Passive Streaming	Uncertain for Active Streaming and Probably NO for Passive Streaming	Probably YES, but exception for active streaming of news. Expert unclear re: passive streaming		Probably YES for active and passive streaming (but no case law or precedents yet)

Question 3c: Stream-ripping copyright-protected content

		Europe							Americas		Asia			
		France	Germany	Netherlands	Poland	Spain	Sweden	United Kingdom	Brazil	Canada	Hong Kong	Indonesia	Japan	Thailand
		FRA	DEU	NLD	POL	ESP	SWE	GBR	BRA	CAN	HKG	IDN	JAP	THA
Exclusive Right	Stream-ripping is restricted act?		same as downloading from unauthorized source	Uncertain (no case law), but probably YES if from unauthorized / illegal sources (= Downloading)	same as downloading from unauthorized source	same as downloading from unauthorized source		same as downloading from unauthorized source	likely but uncertain - not addressed by courts yet	likely but uncertain - not addressed by courts yet	same as downloading from unauthorized source	same as downloading from unauthorized source	same as downloading from unauthorized source	same as downloading from unauthorized source
	under reproduction right?								likely but uncertain - not addressed by courts yet	likely but uncertain - not addressed by courts yet				
	under general exploitation clause?													
	TPM circumvention?	if w/ knowledge, except for research purposes, subject to fine	possible but uncertain (case by case) s. 95a - requires knowledge	possible but uncertain (case by case)	possible but uncertain (case by case)			uncertain but probably not	likely but uncertain, if the ripping involves TPM circumvention	likely but uncertain, if the ripping involves TPM circumvention			YES if a TPM is circumvented (unclear if that's the case) and circumvention is done w/ knowledge	uncertain: certain types of stream ripping may be considered TPM circumvention
	restricted only if knowledge/awareness of illegal/unauthorised source	YES for TPM; NO for REP right	YES for TPM; NO for REP right	NO; <i>TPM not discussed</i>	NO; <i>TPM not discussed</i>	NO; <i>TPM not discussed</i>	NO						YES, apparently for both the REP right and TPM circumvention	NO; <i>TPM not discussed</i>
	restricted only if commercial or for-profit?													NO; <i>TPM not discussed</i>
	Differences per content type?												YES, right applies only to digital sound or visual recordings	
	Legal uncertainty application of right?		NO for REP, but uncertain for TPM	see above (no case law)	NO for REP right; not discussed for TPM		NO for REP; some uncertainty re: <i>TPM</i>		see above (no case law)	see above (no case law)				NO for REP, but uncertain for TPM

Exception	Applicable exception?	Not Discussed (probably not); see 3a Downloading	For REP, PC exception may apply (= downloading); NO exception for TPM circumvention	For REP, PC exception may apply (= downloading)	Possible application of Private use exception (= downloading); NO exception for TPM circumvention		YES, PC exception seems to apply, assuming streaming is from authorized source		Not Discussed; see 3a Downloading	Not Discussed; see 3a Downloading	YES, possible fair dealing defence (for the purpose of research, private study, criticism, review, news reporting, education + reqs of acknowledgment and removal)	general exception / fair dealings clause for non-commercial use (s. 46 © Act).	Yes for REP (private copying); NO for TPM circumvention	Yes for REP (private copying); TPM not discussed
	Applicable if: authorised source?		For REP (PC)	For REP (PC)	Private use uncertain / debated				id	id			For REP (presumed from response)	For REP
	Applicable if: non-commercial use?		For REP (PC)	For REP (PC)					id	id	see above fair dealing		For REP (presumed from response)	For REP (presumed from response)
	Applicable if: knowledge or intent?								id	id				
	Exception remunerated?			YES for REP (PC)					id	id				
	Differences per content type relevant to study?	NO (but: VG as SW not discussed)	NO (but: VG as SW not discussed)	NO (but: VG as SW not discussed)	Exception not applicable to video games (=software)		Exception not applicable to entire books and (probably) VGs (= SW)		id	id				
	Legal uncertainty application exception?				see supra				id	id	case by case	case by case		
	Stream-ripping copyright content (civil) infringing ©?	YES and probably also infringes TPM protection	YES and probably also infringes TPM protection	Probably, if from unauthorized / illegal sources (= Downloading); uncertain if it infringes TPM		YES and probably also infringes TPM protection	NO, if original stream comes from authorized source; YES for entire books; uncertainty on the articulation w/ TPMs and TOS prohibiting streaming	Probably YES for reproduction (but no case law yet); uncertain for TPMs	uncertain (but probably yes)	uncertain (but probably yes)	uncertain (Possible Fair Dealing)	Reproduction: YES, if for commercial purposes. No, if non-commercial. Probably also infringes TPM protection	YES for REP of digital sound or visual recordings; uncertain for TPM	YES for REP; uncertain for TPMs

Question 3d: Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder

Question 3d: Uploading copyright-protected content to a website or online platform accessible to the public without the authorization of the rights holder

		Europe						Americas		Asia				
		France FRA	Germany DEU	Netherlands NLD	Poland POL	Spain ESP	Sweden SWE	United Kingdom GBR	Brazil BRA	Canada CAN	Hong Kong HKG	Indonesia IDN	Japan JAP	Thailand THA
Exclusive Right	Uploading is restricted act?													
	under C2P right?	<i>If underlying REP aimed at subsequent C2P</i>	<i>Making Available</i>		<i>Making Available</i>	<i>Making Available</i>					<i>Making Available</i>	<i>"Public Transmission Right"</i>		
	Under other rights?	<i>Primarily infringing under REP</i>			<i>REP</i>		<i>REP</i>	<i>Possible additional infringement of REP</i>	<i>Probably infringing DISTRIB</i>	<i>REP</i>	<i>REP</i>			
	under general exploitation clause?				<i>? To check relationship w/ typified rights</i>									
	restricted only if knowledge/awareness of illegal/unauthorised source													
	restricted only if commercial or for-profit?													
	Differences per content type?													
	Legal uncertainty application of right?							<i>But: no specific provisions on this</i>			<i>Possible Fair Dealing defence</i>			

Exception	Applicable exception?								YES, for UGC and limited fair dealing user rights (mostly partial reproduction of works for: research, education, parody or satire)	YES, possible fair dealing defence (for the purpose of research, private study, criticism , review, news reporting, education + reqs of acknowledgment and removal)				
	Applicable if: authorised source?													
	Applicable if: non-commercial use?								Yes for UGC (also requires: individual uses) + presumably some fair dealing cases	see above fair dealing				
	Applicable if: knowledge or intent?													
	Differences per content type relevant to study?													
	Legal uncertainty application exception?								see above UGC and fair dealing	see above fair dealing				
	Uploading from illegal/unauthorised source infringing copyright (civil)?	YES (REP + C2P)	YES (C2P, m.a.r)	YES (C2P)	YES (REP + C2P)	YES (C2P, m.a.r)	YES (REP + C2P)	YES (C2P + possible infringement of REP)	YES	YES, unless covered by UGC exception or fair dealing (research, education, parody or satire)	YES, unless covered by fair dealing defence	YES (REP + C2P)	YES (C2P)	YES (C2P)

Question 3e: Posting hyperlinks to copyright-protected content that has been made available online without the express authorization of the rights holder

		Europe							Americas		Asia			
		France	Germany	Netherlands	Poland	Spain	Sweden	United Kingdom	Brazil	Canada	Hong Kong	Indonesia	Japan	Thailand
		FRA	DEU	NLD	POL	ESP	SWE	GBR	BRA	CAN	HKG	IDN	JAP	THA
Exclusive Right	Hyperlinking is restricted act?	Subject to conditions	Subject to conditions	Subject to conditions	Probably follows CJEU Svensson (but absence of case law)	Probably follows CJEU Svensson (but absence of case law)	Subject to conditions	Subject to conditions	NO but possibility of joint liability (solidarity) if link to unauthorized source + for-profit	Probably NO (but courts have not specifically addressed this issue for copyright, only defamation)	Probably (but absence of case law)		Uncertain: Probably NO primary liability but only Secondary Liability	Probably (but absence of case law)
	under C2P right?			if restricted	if restricted	if restricted					if restricted			if restricted
	Under other rights?								For joint liability expert refers to Art 104 Copyright Act, on distribution or other use		Possible that an hyperlink that circumvents technological measures infringes TPM			
	under general exploitation clause?													
	restricted only if knowledge/awareness of illegal/unauthorised source	GS MEDIA CJEU case law	GS MEDIA CJEU case law	GS MEDIA CJEU case law	Probably YES (assuming POL courts follow CJEU case law)	Probably YES (assuming ESP courts follow CJEU case law)	GS MEDIA CJEU case law	GS MEDIA CJEU case law						
	restricted only if commercial or for-profit?	GS MEDIA CJEU case law: linked to knowledge test	GS MEDIA CJEU case law: linked to knowledge test (but: knowledge presumption does not apply to search engines)	GS MEDIA CJEU case law: linked to knowledge test	Probably YES (assuming POL courts follow CJEU case law)	Probably YES (assuming POL courts follow CJEU case law)	GS MEDIA CJEU case law: linked to knowledge test	GS MEDIA CJEU case law: linked to knowledge test	For joint liability (see supra)					
	Differences per content type?													
	Differences per type of linking				Probably NO	Probably NO								
	Legal uncertainty application of right?	Application of knowledge and profit conditions	Application of knowledge and profit conditions (although expert does not mention these)	uncertain whether CJEU case law applies to non-clickable hyperlinks	Application of knowledge and profit conditions + Absence of case law	Application of knowledge and profit conditions	Application of knowledge and profit conditions	Application of knowledge and profit conditions + Absence of case law	But: absence of specific provision on this	But: absence of case law	Absence of case law		See above: Probably NO primary liability but only Secondary Liability	But: absence of case law

Exception	Applicable exception?												
	Applicable if: authorised source?												
	Applicable if: non-commercial use?												
	Applicable if: knowledge or intent?												
	Differences per content type relevant to study?												
	Legal uncertainty application exception?												
	Posting hyperlinks to content available without the authorization of the rights holder (civil)?	Subject to conditions: knowledge + profit / commercial	Subject to conditions: knowledge + profit / commercial (no application of knowledge presumption to search engines)	Subject to conditions: knowledge + profit / commercial	Subject to conditions: knowledge + profit / commercial (but: absence of case law)	Probably YES, but still some uncertainty re: new trend trend of ESP courts post CJEU <i>Svensson</i>	Subject to conditions: knowledge + profit / commercial	Subject to conditions: knowledge + profit / commercial (but: absence of case law)	Probably NO primary liability; Possible joint liability if link to unauthorised source + for-profit	Probably NO	Probably YES re: C2P and possibly TPM circumvention depending on case (but no case law yet)	Probably NO primary liability; Possible secondary liability	Probably YES (but no case law yet)

Question 3f: The sale of Kodiboxes or similar devices, especially when these are sold w/ unauthorized add-ons by default

Question 3f: The sale of Kodiboxes or similar devices, especially when these are sold w/ unauthorized add-ons by default

		France FRA	Germany DEU	Netherlands NLD	Europe Poland POL	Spain ESP	Sweden SWE	United Kingdom GBR	Americas Brazil BRA	Canada CAN	Hong Kong HKG	Asia Indonesia IDN	Japan JAP	Thailand THA
Exclusive Right	Sale of Kodi boxes is restricted act?	Following CJEU	Possible primary infringement following CJEU (but: Absence of case law)	Following CJEU	Possible primary infringement following CJEU (but: Absence of case law)	Uncertain, yet to be assessed by Courts (possible ESP courts follow Filmspeler, but also possible this is deal under Secondary liability)	Probably, if including unauthorized add-ons by default (following CJEU case law)	Probably, if including unauthorized add-ons by default (following CJEU case law)	Probably, if including unauthorized add-ons (applicable to sellers / distributors)	Currently unclear: injunction in place but no final decision in <i>Bell Canada v. 1326030 Ontario Inc. (ITVBox.net)</i>	Probably NO as primary liability / only as Secondary Liability (but: absence of case law)		Probably NO as primary liability / only as Secondary Liability (but: absence of case law)	Subject to conditions
	under C2P right?	Following CJEU		Following CJEU										Making Available
	Under other rights / regimes?	YES: Specific provision Art. L.335-2-1 IPC on provision of software to communicate unauthorized works to public (or encouraging use thereof)	Prior to CJEU <i>Filmspeler</i> , probably Secondary Liability (interferer or contributory liability)	not discussed	Prior to CJEU <i>Filmspeler</i> , probably Secondary Liability (tort of assisting in © infringement)		Possibility of secondary liability	not discussed			Possible secondary liability: authorization (s.22.2 HK Ordinance); Contributory Infringement by common design; Enabling or Facilitation circumvention of TPMs		Possibility of secondary liability	
	under general exploitation clause?													
	restricted only if knowledge/awareness of illegal/unauthorised source	Following CJEU	Possible: Following CJEU (also possible secondary liability)	Following CJEU	Possible: Following CJEU		Probably: Following CJEU	Probably: Following CJEU	Restricted only if device includes unauthorized add-ons					
	restricted only if commercial or for-profit?	Following CJEU	If primary liability applicable post CJEU <i>Filmspeler</i>	Following CJEU	If primary liability applicable post CJEU <i>Filmspeler</i>		If primary liability applicable post CJEU <i>Filmspeler</i>	If primary liability applicable post CJEU <i>Filmspeler</i>	To extent that act is be definition commercial					
	Differences per content type?													
	Legal uncertainty application of right?		see above		see above	see above	see above	Some uncertainty due to lack of case law and the requirements for primary liability in this scenario	re: restriction in general + type of right involved)		See above: possible secondary liability + absence of case law		See above: possible secondary liability + absence of case law	

Exception	Applicable exception?									
	Applicable if: authorised source?									
	Applicable if: non-commercial use?									
	Applicable if: knowledge or intent?									
	Differences per content type relevant to study?									
	Legal uncertainty application exception?									

Question 3: Summary Table

	Europe							Americas		Asia			
	France FRA	Germany DEU	Netherlands NLD	Poland POL	Spain ESP	Sweden SWE	United Kingdom GBR	Brazil BRA	Canada CAN	Hong Kong HKG	Indonesia IDN	Japan JAP	Thailand THA
Downloading from illegal/unauthorised source infringing copyright (civil)?				Yes for video games, but unclear for other content				Probable but uncertain	YES, except for musical sound recordings (apparently non-infringing)	Possible Fair Dealing	YES, if for commercial purposes. No, if non-commercial	YES (for digital sound or visual recordings)	
Streaming from illegal/unauthorised source infringing copyright (civil)?	If through unauthorized kodi box	Probably, but uncertain application of Temp/Transient exception	YES, at least through unauthorized kodi box (uncertain application to other passive streaming scenarios)			Probably YES after CJEU Filmspeler, but no case law yet and prior situation exempted these uses under Temp/Transient exception		Yes for Active Streaming and Uncertain / unlikely for Passive Streaming	YES for Active Streaming and Probably NO for Passive Streaming	Uncertain for Active Streaming and Probably NO for Passive Streaming	Probably YES, but exception for active streaming of news. Expert unclear re: passive streaming		Probably YES for active and passive streaming (but no case law or precedents yet)
Stream-ripping copyright content (civil) infringing ©? [Assumption: lawful/unauthorized source]	YES and probably also infringes TPM protection	YES and probably also infringes TPM protection	Probably, if from unauthorized / illegal sources (= Downloading); uncertain if it infringes TPM		YES and probably also infringes TPM protection	NO, if original stream comes from authorized source; YES for entire books; uncertainty on the articulation w/ TPMs and TOS prohibiting streaming	Probably YES for reproduction (but no case law yet); uncertain for TPMs	uncertain (but probably yes)	uncertain (but probably yes)	uncertain (Possible Fair Dealing)	Reproduction: YES, if for commercial purposes. No, if non-commercial. Probably also infringes TPM protection	YES for REP of digital sound or visual recordings; uncertain for TPM	YES for REP; uncertain for TPMs
Uploading from illegal/unauthorised source infringing copyright (civil)?	YES (REP + C2P)	YES (C2P, m.a.r)	YES (C2P)	YES (REP + C2P)	YES (C2P, m.a.r)	YES (REP + C2P)	YES (C2P + possible infringement of REP)	YES	YES, unless covered by UGC exception or fair dealing (research, education, parody or satire)	YES, unless covered by fair dealing defence	YES (REP + C2P)	YES (C2P)	YES (C2P)
Posting hyperlinks to content available without the authorization of the rights holder (civil)?	Subject to conditions: knowledge + profit / commercial	Subject to conditions: knowledge + profit / commercial (no application of knowledge presumption to search engines)	Subject to conditions: knowledge + profit / commercial	Subject to conditions: knowledge + profit / commercial (but: absence of case law)	Probably YES, but still some uncertainty re: new trend trend of ESP courts post CJEU Svensson	Subject to conditions: knowledge + profit / commercial	Subject to conditions: knowledge + profit / commercial (but: absence of case law)	Probably NO primary liability; Possible joint liability if link to unauthorised source + for-profit	Probably NO	Probably YES re: C2P and possibly TPM circumvention depending on case (but no case law yet)		Probably NO primary liability; Possible secondary liability	Probably YES (but no case law yet)
Sale of kodi boxes w/ unauthorized add-ons by default infringing (c) (civil)?	YES for C2P (subject to conditions: knowledge + profit or commercial) + YES for specific regime described of Art. L.335-2-1 IPC)	Probably, following CJEU but uncertain (otherwise, secondary liability would apply)	YES for C2P (subject to conditions: knowledge + profit or commercial)	Probably, following CJEU	Uncertain: absence of case law; possible ESP courts follow CJEU but also possible act qualifies under Secondary liability	If including unauthorized add-ons by default (following CJEU); but also possible Secondary liability	If including unauthorized add-ons by default (following CJEU)	Probably, if the device contains unauthorized add-ons	Currently unclear: injunction in place but no final decision in <i>Bell Canada v. 1326030 Ontario Inc. (iTVBox.net)</i>	Probably NO primary liability, but possible secondary liability (authorization, contributory, enabling/facilitating circumvention)		Probably NO primary liability	YES for C2P (subject to conditions: knowledge + profit or commercial)



LEGISLATION AND CASES

International

- BC:** Berne Convention for the Protection of Literary and Artistic Works, of 9 September 1886 (completed at Paris on 4 May 1896, revised at Berlin on 13 November 1908, completed at Berne on 20 March 1914, revised at Rome on 2 June 1928, at Brussels on 26 June 1948, at Stockholm on 14 July 1967, and at Paris on 24 July 1971, and amended on 28 September 1979)
- RC:** International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations, done at Rome on October 26, 1961
- TRIPS:** Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, The Legal Texts: The Results of The Uruguay Round Of Multilateral Trade Negotiations 320 (1999), 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994)
- WCT:** WIPO Copyright Treaty, adopted in Geneva on 20 December 1996
- WPPT:** WIPO Performances and Phonograms Treaty, adopted in Geneva on December 20, 1996
- WTO Agreement:** WTO Agreement: Marrakesh Agreement Establishing the World Trade Organization, 15 April 1994, The Legal Texts: The Results of The Uruguay Round Of Multilateral Trade Negotiations 4 (1999), 1867 U.N.T.S. 154, 33 I.L.M. 1144 (1994)

European Union

EU Treaties and Charter

- Charter:** Charter of Fundamental Rights of the European Union, OJ C 364/1, 18.12.2000.
- TEU:** Treaty on European Union (Consolidated Version), Treaty of Maastricht, 7 February 1992, OJ EC C 325/5; 24 December 2002
- TFEU:** Consolidated Version of the Treaty on the Functioning of the European Union, Sep. 5, 2008, 2008 O.J. (C 115) 47

EU Directives

- CRM Directive:** Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market, OJ L 84, 20.3.2014, p. 72–98.
- Database Directive:** Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77/20, 27.03.1996.
- E-Commerce Directive (ECD):** 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, 17.7.2000, p. 1–16
- Enforcement Directive:** 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, 30.04.2004.
- InfoSoc Directive:** Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167/10, 22.06.2001.
- Orphan Works Directive:** Directive 2012/28/EU of the European Parliament and of the Council of 25 October 2012 on certain permitted uses of orphan works.
- Rental and Lending Rights Directive:** Council Directive 92/100/EEC, of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual

property, 1992 O.J. (L 346/61) as republished and amended by Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 (codified version), 2006 O.J. (L 376/28).

Resale Right Directive: Directive 2001/84/EC of the European parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art, OJ L 272/32, 13.10.2001.

SatCab Directive: Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, OJ L 248/15, 6.10.1993.

Software Directive: Council Directive 91/250/EEC, of 14 May 1991 on the legal protection of computer programs, 1991 O.J. (L 122/42), as republished and amended by Directive 2009/24/EC, of the European Parliament and of the Council of 23 April 2009 (codified version), 2009 O.J. (L 111/16).

Term Directive: Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights, 2006 O.J. (L 372/12), as amended by Directive 2011/77/EU of the European Parliament and of the Council of 27 September 2011, 2011 O.J. (L 265/1)

EU Proposed Legislation

Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM(2016)593

Table of Cases Court of Justice Of The European Union (CJEU)

ACI Adam: Case C-435/12, ACI Adam BV and Others v Stichting de Thuiskopie and Stichting Onderhandeligen Thuiskopie vergoeding, 10.04.2014, ECLI:EU:C:2014:254

Airfield: Joined Cases C-431/09 and C-432/09, Airfield NV and Canal Digitaal BV v Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (Sabam) (C-431/09) and Airfield NV v Agicoa Belgium BVBA (C-432/09), 13.10.2011, ECLI:EU:C:2011:157

BestWater: Case C-348/13, BestWater International GmbH v Michael Mebes and Stefan Potsch, 21.10.2014, ECLI:EU:C:2014:2315 (Order)

Bonnier Audio: Case C-461/10, Bonnier Audio AB and Others v Perfect Communication Sweden AB, 19.04.2012, ECLI:EU:C:2012:219

Circul Globus: Case C-283/10, Circul Globus București (Circ & Variete Globus București) v Uniunea Compozitorilor și Muzicologilor din România – Asociația pentru Drepturi de Autor (UCMR – ADA), 24.11.2011, ECLI:EU:C:2011:772

C More Entertainment: Case C-279/13, C More Entertainment AB v Linus Sandberg, 26.03.2015, ECLI:EU:C:2015:199

Coditel I: Case 62/79, SA Compagnie générale pour la diffusion de la télévision, Coditel, and others v Ciné Vog Films and others, 19.03.1980, ECLI:EU:C:1980:84

Coditel II: Case 262/81, Coditel SA, Compagnie générale pour la diffusion de la télévision, and others v Ciné-Vog Films SA and others, ECJ 6.10.1982, ECLI:EU:C:1982:334

Donner: Case C-5/11, Criminal proceedings against Titus Alexander Jochen Donner, 21.06.2012, ECLI:EU:C:2012:370

DR and TV2 Danmark: Case C-510/10, DR and TV2 Danmark A/S v NCB - Nordisk Copyright Bureau, 26.04.2012, ECLI:EU:C:2012:244

EGEDA I: Case C-293/98, Entidad de Gestión de Derechos de los Productores Audiovisuales (Egeda) v Hostelería Asturiana SA (Hoasa), 03.02.2000, ECLI:EU:C:2000:66

Filmspeler: Case C-527/15, Stichting BREIN v Jack Frederik Wullums, 26.04.2017, ECLI:EU:C:2017:300

Google France/Louis Vuitton: Joined Cases C-236/08, C-237/08 and C-238/08, Google France SARL, Google Inc. v Louis Vuitton Malletier SA, Google France SARL v Viaticum SA, Luteciel SARL and Google France SARL v Centre national de recherche en relations humaines

- (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL, 23.03.2010, ECLI:EU:C:2010:159
- GS Media:** Case C-160/15, GS Media BV v Sanoma Media Netherlands BV and Others, 8.09.2016, ECLI:EU:C:2016:644
- Infopaq I:** Case C-5/08, Infopaq International A/S v Danske Dagblades Forening, 16.07.2009, ECLI:EU:C:2009:465
- Infopaq II:** Case C-302/10, Infopaq International A/S v Danske Dagblades Forening, 17.01.2012 (Order), ECLI:EU:C:2012:16
- ITV Broadcasting:** Case C-607/11, ITV Broadcasting Ltd v TVCatchUp Ltd, 07.03.2013, ECLI:EU:C:2013:147
- Lagardère :** Case C-192/04, Lagardère Active Broadcast v Société pour la perception de la rémunération équitable (SPRE) and Gesellschaft zur, 14.07.2005, ECLI:EU:C:2005:475
- Laserdisken II:** Case C-479/04, Laserdisken ApS v Kulturministeriet, 12.09.2006, ECLI:EU:C:2006:549
- Liffers:** Case C-99/15, Christian Liffers v Producciones Mandarina SL and Mediaset España Comunicación SA, anciennement Gestevisión Telecinco SA, 17.03.2016, ECLI:EU:C:2016:173
- L'Oréal/eBay:** Case 324/09, L'Oréal SA and Others v eBay International AG and Others, 12.07.2011, ECLI:EU:C:2011:474
- LSG:** Case C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH, 19.02.2009, ECLI:EU:C:2009:107
- Luksan:** Case C 277/10, Martin Luksan v Petrus van der Let, 9.02.2012, ECLI:EU:C:2012:65
- Murphy:** Joined Cases C-403/08 and C-429/08, Football Association Premier League Ltd and Others v QC Leisure and Others (C-403/08) and Karen Murphy v Media Protection Services Ltd (C-429/08), 4.10.2011, ECLI:EU:C:2011:631
- Netlog:** Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, 16.02.2012, ECLI:EU:C:2012:85
- Nintendo:** Case C-355/12, Nintendo Co. Ltd and Others v PC Box Srl and 9Net Srl, Case 23.01.2014, ECLI:EU:C:2014:25
- OSA:** Case C-351/12, OSA - Ochranný svaz autorský pro práva k dílům hudebním o.s. v Léčebné lázně Mariánské Lázně a.s., 27.02.2014, ECLI:EU:C:2014:110
- Organismos Sillogikis:** Case C-136/09, Organismos Sillogikis Diacheirisis Dimiourgon Theatrikon kai Optikoakoustikon Ergon v Divani Akropolis Anonimi Xenodocheiaki kai Touristiki Etaireai, 18.03.2010, ECLI:EU:C:2010:151 (Order)
- Painer:** Case C-145/10, Eva-Maria Painer tegen Standard VerlagsGmbH en anderen, 1.12.2011, ECLI:EU:C:2011:798
- Papasavvas:** Case C-291/13, Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi and Giorgos Sertis, 11.09.2014, ECLI:EU:C:2014:2209
- Peek & Cloppenburg:** Case C-456/06, Peek & Cloppenburg KG v Cassina SpA, 17.04.2008, ECLI:EU:C:2008:232
- PPI:** Case C-162/10, Phonographic Performance (Ireland) Limited v Ireland and Attorney General, 15.03.2012, ECLI:EU:C:2012:141
- Promusicae:** Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, 29.01.2008, ECLI:EU:C:2008:54
- Rafael Hoteles:** Case C-306/05, Sociedad General de Autores y Editores de España (SGAE) v Rafael Hoteles SA, 07.12.2006, ECLI:EU:C:2006:764
- Reha Training:** Case C-117/15, Reha Training Gesellschaft für Sport- und Unfallrehabilitation mbH v Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (GEMA), 31.05.2016, ECLI:EU:C:2016:379
- SAS:** Case C-406/10, SAS Institute Inc. v World Programming Ltd, 02.05.2012, ECLI:EU:C:2012:259
- SBS:** Case C-325/14, SBS Belgium NV v Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM), 19.11.2015, ECLI:EU:C:2015:764
- Scarlet Extended:** Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 24.11.2011, ECLI:EU:C:2011:771

- SCF:** Case C-135/10, Società Consortile Fonografici (SCF) v Marco Del Corso, 15.03.2012, ECLI:EU:C:2012:140
- Sociedade Portuguesa de Autores:** Case C-151/15, Sociedade Portuguesa de Autores v Ministério Público and Others, 14.07.2015, ECLI:EU:C:2015:468 (Order)
- Svensson:** Case C-466/12, Nils Svensson v Retriever Sverige AB, 13.02.2014, ECLI:EU:C:2014:76
- UPC Telekabel:** Case C-314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH, 27.03.2014, ECLI:EU:C:2014:192
- UsedSoft:** Case C-128/11, UsedSoft GmbH v Oracle International Corp., 3.07.2012, ECLI:EU:C:2012:407
- VOB:** Case C-174/15, Vereniging Openbare Bibliotheken v Stichting Leenrecht, 10.11.2016, ECLI:EU:C:2016:856
- Ziggo:** Case C-610/15, Stichting Brein v Ziggo, 14.06.2017, ECLI:EU:C:2017:456