DOI 10.5817/MUJLT2023-2-3

ADDRESSING EVOLVING DIGITAL PIRACY THROUGH CONTRIBUTORY LIABILITY FOR COPYRIGHT INFRINGEMENT: THE MOBDRO CASE STUDY

by

MINDAUGAS KIŠKIS *

Digital piracy, i.e., large-scale commercial copyright infringement online, is a constantly evolving phenomenon. Following the enactment and expansion of online intermediary liability rules, professional pirates have shifted away from easily blockable websites and services. Streaming piracy on dedicated platforms, monetised through embedded services, has become the prevalent model in Europe, as is well illustrated by the Mobdro case study analysed in this article. These dedicated platforms are supported by embedded service providers who, as they are not online intermediaries, can avoid the online intermediary liability regime. One potential solution to this issue could be the application of contributory copyright infringement rules, which are well-established in US copyright law but absent in EU law, to all parties that contribute to digital piracy. The CJEU has opened expressly this path in the recent C-682/18 YouTube and C-683/18 Cyando cases. Based on the CJEU's initiative and the existing precedent of harmonising intellectual property tort rules within EU law, further contributory liability rules could be modelled after US rules by updating the Enforcement Directive 2004/48/EC. Addressing this gap in EU copyright law is crucial for enhancing the effectiveness of digital copyright enforcement against evolving digital piracy.

KEY WORDS

Copyright, Contributory liability, Piracy, Streaming, Embedded SDK

* mkiskis@mruni.eu, Professor, Faculty of Public Governance and Business & MRU Law School, Mykolas Romeris University, Lithuania

1. INTRODUCTION

General legal liability principles of criminal and tort law in modern legal systems suggest that liability for unlawful action causing damage shall apply not only to direct infringers, but also to parties who contribute to the infringement. There are no material reasons why substantive copyright law should apply different liability principles, but for various historical reasons the liability rules for copyright infringements vary significantly in different jurisdictions. The US substantive copyright law has developed a thorough concept of secondary civil liability for copyright infringements, the two main branches of which are contributory liability and vicarious liability; however, substantive copyright laws in Europe are rather shy in regulating indirect copyright infringement and legal liability for it. European scholars have also not adopted a uniform concept or nomenclature for secondary liability for copyright infringement, with some resorting to overly narrow interpretations[1] which may exclude contributors from secondary liability for copyright infringement. This is representative of the overwhelming focus of European jurisprudence on the liability of online intermediaries, which may prove increasingly insufficient in view of recent directions in the evolution of digital piracy, i.e., large-scale commercial copyright infringement online.

In one of the most famous copyright enforcement cases in the EU – the Pirate Bay criminal cases in Sweden – the operators of the Pirate Bay website were all convicted not for direct or primary copyright infringement, but rather for aiding and abetting copyright infringement performed by others.[2] The crime of the Pirate Bay operators was contributing to the copyright infringement committed by the users of the Pirate Bay. The Pirate Bay perpetrators were found liable for the civil damages caused to

[1] See, e.g., the definition of "secondary liability" in Husovec, M. (2013) Injunctions against Innocent Third Parties: The case of Website Blocking. *JIPITEC*, 4, p. 118, para. 11, note 4 – the statement that "Secondary liability could be further divided into fault-based secondary liability that requires the breach of a certain duty of care, and no-fault-based secondary liability that triggers liability regard-less of such a breach" excludes contributory liability as it is understood in US common law, i.e., fault-based secondary liability that requires inducing or material contribution to the activity of the direct infringer. "Fault-based secondary liability that requires the breach of a certain duty of care" according to US common law would imply vicarious liability only. For comparison, on the US common law doctrine of "secondary liability for copyright infringement" see Folsom, T. C. (2009) Toward Non-Neutral Principles of Private Law: Designing Secondary Liability Rules for New Technological Uses. *Akron Intellectual Property Journal*, 3, pp. 45, 52, and Mehra, S. K. (2011) Keep America Exceptional! Against Adopting Japanese and European-Style Criminalization of Contributory Copyright Infringement. *Vanderbilt Journal of Entertainment and Technology Law*, 13 (4), which clearly differentiate "contributory liability" and "vicarious liability", which are separate from faultless secondary liability.

[2] Kravets, D. (2009) *English Transcript of Pirate Bay Guilty Verdicts Released*. Wired. Available from: `https://www.wired.com/2009/04/english-transcript-of-pirate-bay-guilty-verdicts-released/`

the rightsholders; however, these tort claims were resolved as part of the criminal cases, which lasted for almost a decade, and not through separate civil action procedures, which may have been simpler and faster. More than a decade later, civil action against a perpetrator who did not violate copyright themselves and who is not an online intermediary remains a murky topic in European copyright law.

On the one hand, the Electronic Commerce Directive 2000/31/EC, the InfoSoc Directive 2001/29/EC, and the Enforcement Directive 2004/48/EC introduced special rules on the secondary liability of and injunctions against internet intermediaries,[3] which were inspired by the substantively similar earlier rules in US copyright law (the 1998 Digital Millennium Copyright Act) and the TRIPS agreement. On the other hand, secondary liability rules remain generally absent with respect to parties who are not explicit online intermediaries. This gap in the liability and infringement rules of European copyright law is most apparent in comparison to US copyright law. To a certain extent, this gap already manifested in European copyright liability case law, where the attempt was made to address secondary liability for copyright infringement through the stretched interpretation of the right to communicate to the public, or by imaginative applications of obscure national tort law doctrines, which have only indirect relationships to, and no statutory basis in, copyright (e.g., Störerhaftung in Germany).

European jurisprudence on the issue of secondary liability for copyright infringement predominantly focusses on issues of online intermediary liability and injunctions against intermediaries.[4] A substantial body of work addresses trademark-specific issues: mainly injunctions against platforms for offering counterfeit goods, which has been the subject matter of multiple cases at the Court of Justice of the European Union (CJEU).[5] The research acknowledges that secondary liability actions are most prevalent in cases involving digital content, which also includes copyrighted material.[6] It is also notable that existing comparative analyses of intermediary liability issues in the EU,[7] including rare work that focusses on European intermediary

[3] Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press, pp. 42–46.

[4] Frosio, G. (ed.) (2020) *Oxford Handbook of Online Intermediary Liability*. Oxford: OUP.

[5] Dinwoodie, G., Dreyfuss, R., and Kur, A. (2009) The Law Applicable to Secondary Liability in Intellectual Property Cases. *New York University Journal of International Law and Politics*, 2, pp. 201–235. Available from: `https://nyujilp.org/wp-content/uploads/2013/02/42.1-Dinwoodie-Dreyfuss-Kur.pdf`

[6] *Op. cit.*, p. 204.

[7] Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, Available from: `https://doi.org/`

liability in copyright,[8] are limited only to German and French law, which are not representative of the whole of the EU. All aforementioned research recognises that secondary liability is important for the effective enforcement of intellectual property online, and urges the further harmonisation of rules at the EU level.[9] This is crucial in the context of digital piracy, which is an inherently cross-border phenomenon and requires supranational legal rules to address it. Digital piracy is also a very dynamic and rapidly evolving phenomenon, which is shall studied by looking at very recent examples, such as the Mobdro case study presented in this article. This case study illustrates how piracy platforms are avoiding online intermediary liability and monetising their activities through the embedded services model, thus making it difficult for rightsholders to pursue damages. Embedded service providers themselves are not online intermediaries – at least not in the traditional sense – and therefore their activities cannot be addressed through online intermediary liability rules, allowing them to slip through the legal gaps of copyright infringement liability rules, at least in Europe.

There are no existing EU legal research articles specifically addressing the secondary liability of non-intermediary parties that are instrumental and material contributors to copyright infringement. To address the particularities of this aspect, in the authors' opinion it is preferable to use the term *contributory liability* for copyright infringement, rather than the general term *secondary liability*.[10] Although secondary liability in the context of digital piracy is little-explored in European legal research, in the US it has been one of the main topics of secondary liability for copyright infringement,[11] particularly focusing on contributory liability. Some US scholars specifically highlight the advantages of the civil law enforcement

10.1093/jiplp/jpt213, and Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press.

8 Angelopoulos, C. (2016) *European Intermediary Liability in Copyright: A Tort-Based Analysis*. Wolters Kluwer.

9 Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press, pp. 42–46., Dinwoodie, G., Dreyfuss, R., and Kur, A. (2009) The Law Applicable to Secondary Liability in Intellectual Property Cases. *New York University Journal of International Law and Politics*, 2, pp. 201–235. Available from: https://nyujilp.org/wp-content/uploads/2013/02/42.1-Dinwoodie-Dreyfuss-Kur.pdf, Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, Available from: https://doi.org/10.1093/jiplp/jpt213, Angelopoulos, C. (2016) *European Intermediary Liability in Copyright: A Tort-Based Analysis*. Wolters Kluwer.

10 Differences between the two are discussed in note 1. Also, note that the term of contribution to infringement ("*contributes [...] in breach of copyright*") was recently introduced by the CJEU in judgement in joined cases C-682/18 and C-683/18, par. 102, which is analysed below in the article.

11 Lemley, M. A., and Reese, R. A. (2004) Reducing Digital Copyright Infringement Without Restricting Innovation. *Stanford Law Review*, 56 (6), pp. 1345–1434.

of contributory liability for copyright infringement vis-à-vis contributory liability under criminal law, and argue that criminal prosecution could have a chilling effect on innovation in technologies with "lawful promise".[12] Nevertheless, even in the US secondary liability for copyright infringement has not been investigated in the context of novel digital piracy models.

The purpose of this article is to fill the identified research gap: the lack of proper secondary liability for copyright infringement rules with respect to parties who are not online intermediaries. Through a specific case study, it will be demonstrated how this may be driving online digital piracy in Europe.

The first section of the article briefly comparatively analyses the law relevant to contributory liability for copyright infringement in the EU and the US. Note that the analysis in this article is limited only to copyright law. The second section discusses the changes in digital piracy "business models" over the last two decades and highlights the embedded services model as the current default. The third section examines the Mobdro case study as a recent example of modern dedicated piracy platforms, and analyses it in the context of copyright infringement rules. In the conclusions, the authors argue in favour of proper statutory rules on contributory infringement in the EU, which are crucial for enhancing the effectiveness of digital copyright enforcement against evolving digital pirates.

2. THE LEGAL CONTEXT OF CONTRIBUTORY COPYRIGHT INFRINGEMENT

From a legal perspective, digital piracy is the act of illegal public performance, distribution and reproduction of copyrighted works on the internet, which gives rise to the legal liability of the parties involved. Liability shall generally apply not only to the direct infringer, but also to parties who contribute to the infringement and indirectly infringe copyright, yet European statutory copyright law contains few rules dealing with contributory copyright infringement and collaborators' liability for copyright infringement.

In US copyright law, rightsholders enjoy a century-old doctrine of contributory copyright infringement, a form of secondary liability that makes one party liable for the harm caused by another. According to this case law doctrine, US copyright law thus allows rightsholders to seek relief from all parties who have materially contributed to the copyright infringement. Notably, secondary liability for copyright infringement is a general and

[12] Mehra, S. K. (2011) Keep America Exceptional! Against Adopting Japanese and European-Style Criminalization of Contributory Copyright Infringement. *Vanderbilt Journal of Entertainment and Technology Law*, 13 (4).

autonomous doctrine of US federal copyright law, which is independent from state tort law doctrines, such as the doctrine of tortious interference, which is an autonomous doctrine of tort law in many US states. For context, it is important to bear in mind that copyright law is an exclusive matter of federal jurisdiction in the US, while tort law, with the exception of specific torts (e.g., environmental damage), is a matter of state law. Therefore, copyright law and tort law doctrines generally do not intersect.

EU substantive copyright law is quasi-federal in that it has been very significantly harmonised through the EU Acquis and overrides pertinent national law. Nevertheless, there is no general concept or doctrine of secondary liability for copyright infringement in EU copyright law. One of the main sources of EU substantive copyright law – InfoSoc Directive 2001/29/EC – expressly discusses inducing, enabling, facilitating or concealing an infringement only in the very specific context of rights management (DRM) information (Art. 7(1)), and separately provides for the possibility of intermediary liability (Art. 8(2)) and injunctions against intermediaries (Art. 8(3)). Liability rules for online intermediaries were first introduced in E-Commerce Directive 2000/31/EC (Art. 12-15), and originally meant internet service providers, but gradually expanded in their interpretation to include all online intermediaries, such as online service providers and online platforms that host or convey third party data. Injunction rules are further elaborated with respect to all forms of intellectual property in the Enforcement Directive 2004/48/EC (Art. 9(1) and Art. 11). Note that none of these rules apply to parties who cannot be considered online intermediaries.

Directive 2001/29/EC does not provide for a general definition of copyright infringement, and does not expressly mention secondary or contributory liability. Theoretically, one could argue that this does not preclude secondary liability for copyright infringement as it allows for national rules with higher protection standards (i.e., stricter), but this is then entirely left out for the national law of the Member States. The statutory copyright laws of many EU Member States (which at least include Lithuania, Latvia, Estonia, Poland, Finland, and Germany) follow the same pattern – there are no express statutory provisions on contributory copyright liability, save for specific and limited rules pertaining to the DRM, intermediary liability, and injunctions against online intermediaries based on the national implementation of the aforementioned EU Directives. Theoretically, contributory liability for copyright infringement may be invoked in national law on the basis of various doctrines of national tort law, but this puts a heavy burden on the shoulders of the judiciary and

requires judicial bravery, creativity and activism, which is unlikely in courts of lower instance and is not a very attractive proposition for both judges and rightsholders seeking quick and efficient copyright infringement relief. Unsurprisingly, at least in some countries (for example, Lithuania), there is not a single copyright liability case where secondary liability of a non-online intermediary would be attempted. In other countries (Germany), the lack of statutory contributory infringement rules in national copyright law is somewhat compensated for in the higher instance courts by applying earlier precedents from trademark and patent law cases based on the historical tort law doctrine of Störerhaftung,[13] which is roughly equivalent to the abovementioned US state common law doctrine of tortious interference, but is historically applied in cases of trademark and patent law in Germany.

As was noted, existing comparative analyses of online intermediary liability issues in EU jurisdictions is limited to German and French law[14]; however, the paths taken in these two jurisdictions are complex, specific to the legal traditions of these particular countries, and reliant on decades of case law. The original sources on the pertinent doctrines are not even available in English, the *lingua franca* of Europe. Therefore, transferring this approach to other parties is problematic. In the absence of EU-level rules, differences in national law would inevitably result in substantively different liability outcomes, which is not desirable and may also lock contributory liability enforcement attempts within a jurisdictional maze. None of this would be an issue if indirect copyright infringement or contribution to infringement were explicated in substantive copyright law at the EU level.

The liability of contributors to digital piracy must be addressed at the supranational level, because digital piracy or large-scale commercial copyright infringement online is an inherently cross-border phenomenon that cannot be addressed through national laws alone. This is already recognised at the EU level through efforts to harmonise some intellectual property tort

[13] Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, Available from: https://doi.org/10.1093/jiplp/jpt213, and Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press.

[14] Dinwoodie, G., Dreyfuss, R., and Kur, A. (2009) The Law Applicable to Secondary Liability in Intellectual Property Cases. *New York University Journal of International Law and Politics*, 2, pp. 201–235. Available from: https://nyujilp.org/wp-content/uploads/2013/02/42.1-Dinwoodie-Dreyfuss-Kur.pdf, Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, Available from: https://doi.org/10.1093/jiplp/jpt213, and Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press., Angelopoulos, C. (2016) *European Intermediary Liability in Copyright: A Tort-Based Analysis*. Wolters Kluwer.

rules, most notably the Enforcement Directive 2004/48/EC, yet the lack of comprehensive contributory liability rules is apparent.

Because limited substantive rules on contributory liability are already included in EU law and further harmonisation has already been advocated for and substantiated in existing research,[15] this paper will not discuss whether contributory liability is compatible with the Treaty on the Functioning of the European Union and the Treaty on European Union. The purpose of this article is to highlight the lack of secondary liability for non-online intermediaries in substantive European copyright law, which in the authors' opinion is a critical gap in view of evolving digital piracy models.

It is also noteworthy that the statutory intermediary liability rules and obligations have recently been expanded through the introduction of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act (DSA)). Therefore, it is time to revisit and comprehensively address other copyright liability questions that have been side-lined for the last decade.

Despite some statutory uncertainties, copyright case law in the US has addressed the matter of contributing to copyright infringement with a long-standing doctrine of contributory copyright infringement. This doctrine was introduced by the US courts in 1911 (*Kalem Co. v. Harper Bros.*, 222 U.S. 55, 63 (1911)),[16] and its modern version allows intellectual property rightsholders to seek relief not only from direct infringers, but also from those who somehow knew of and materially contributed to infringing behaviour (*Gershwin Publishing Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971)). To establish contributory infringement, it must first be shown that the party had knowledge of the infringement of the right by another. Second, the party must materially contribute to the infringement. If it was reasonable for the defendant to think that infringement was taking place, the

[15] Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press, pp. 42–46, Dinwoodie, G., Dreyfuss, R., and Kur, A. (2009) The Law Applicable to Secondary Liability in Intellectual Property Cases. *New York University Journal of International Law and Politics*, 2, pp. 201–235. Available from: `https://nyujilp.org/wp-content/uploads/2013/02/42.1-Dinwoodie-Dreyfuss-Kur.pdf`, Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, Available from: `https://doi.org/10.1093/jiplp/jpt213`, Angelopoulos, C. (2016) *European Intermediary Liability in Copyright: A Tort-Based Analysis*. Wolters Kluwer.

[16] Davis Powell, C. (2009) The Saga Continues: Secondary Liability for Copyright Infringement Theory, Practice and Predictions. *Akron Intellectual Property Journal*, 3 (1), Article 7. Available from: `https://ideaexchange.uakron.edu/akronintellectualproperty/vol3/iss1/7`

knowledge standard is satisfied. Moreover, a party that suspects wrongdoing and fails to investigate will also be deemed to satisfy the knowledge standard.

Although this doctrine was not expressly codified into the 1976 US Copyright Law, the U.S. Supreme Court has argued in follow-up cases that the "*absence of such express language in the copyright statute does not preclude the imposition of liability for copyright infringements on certain parties who have not themselves engaged in the infringing activity*" (*Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 104 S. Ct. 774 (1984)). The *Sony* precedent remains pivotal in establishing the requirement and limitations of secondary liability for copyright infringement. In *Sony*, the Court explained that "*[t]he sale of copying equipment, like the sale of other articles of commerce does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses*" – thus essentially establishing safe-harbour exceptions from liability. Nevertheless, a party who knowingly induces, causes or materially contributes to copyright infringement by another person, but who has not committed or participated in the infringing acts themselves, may be held liable as a contributory infringer if they had knowledge, or reason to know, of the infringement. It is very important to note that Sony was not historically an online intermediary, but rather a hardware provider, and the US doctrine of secondary liability for copyright infringement has evolved without even considering the operational technicalities of the internet and the role that online intermediaries play in it.

Contributory liability for copyright infringement doctrine was essential and central in order for US copyright law to effectively address the challenge of peer-to-peer (P2P) copyright piracy starting with Napster (*A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th. Cir., 2001)). This later extended to P2P network operators such as Aimster, Morpheus, Kazaa and Grokster, who attempted to technologically evade liability by increasingly distancing themselves from direct infringement and claiming safe-harbour exceptions according to *Sony*. The 2005 case of *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), where the doctrine of contributory infringement was addressed by the US Supreme Court, currently serves as the penultimate digital piracy precedent case of US copyright law. *Grokster* established that a maker or distributor of software with the object of promoting its use to infringe copyright is liable for the resulting acts of copyright infringement, even though the Grokster program was capable of substantial non-infringing uses. Grokster met the requirements for contributory liability because it induced copyright infringement, and this constituted material contribution to the copyright infringement committed by the users of Grokster. The

inducement rule foresees liability for purposeful, culpable expression and conduct aimed at copyright infringement. US scholars argue that the court based this interpretation of contributory liability on the patent infringement rules,[17] even though the Supreme Court did not mention this themselves. The notion of contributory inducement was further supported by Grokster aiming its technology towards known infringers, and receiving financial benefit from the infringing activities, all of which demonstrated unlawful intent.[18] Such intent towards infringement disqualified Grokster from defence involving the application's substantial noninfringing uses.[19]

A summary of the current US rules is provided in the instructions given to federal civil law jury members on matters of contributory infringement of copyright law.[20] In order for a contributor to be liable for copyright infringement, both of the following elements need to be established by a preponderance of evidence:

> *1) the contributor knew or had reason to know of the infringing activity of a direct infringer; and*
>
> *2) the contributor intentionally induced or materially contributed to the infringer's direct infringing activity. The contributor's intent to induce the infringing activity must be shown by clear expression of that intent or other affirmative steps taken by contributor.*

The requirement for knowledge of the infringement is met if the party is notified of the infringement. The reason to know standard is met if the infringement is reported in the public media or the contributor failed to perform due diligence where it would have been reasonable.

It is not clarified what would be considered material contribution, and in the US courts this is addressed on a case-by-case basis according to the available evidence. According to commentators,[21] material contribution shall be quantified in the context of the relationship between the contributor and the direct infringer, and independently between the contributor and the actual act of infringement. Contributions which modify and aggravate the

---

17 *Ibid.*

18 *Ibid.*

19 Bartholomew, M., and McArdle, P. F. (2011) Causing infringement. *Vanderbilt Law Review*, 64 (3), pp. 675–746.

20 Ninth Circuit Jury Instructions Committee. (2017) 17.21. Derivative Liability—Contributory Infringement—Elements and Burden of Proof. In: *Manual of Model Civil Jury Instructions* [online]. Available from: `https://www.ce9.uscourts.gov/jury-instructions/node/279`[Accessed 28 November 2022].

21 Tilly, J. M. (2008) Perfect 10 v. Visa: the future of contributory copyright infringement. *Oklahoma Law Review*, 61 (4), pp. 865–890; Bartholomew, M., and McArdle, P. F. (2011) Causing infringement. *Vanderbilt Law Review*, 64 (3), pp. 675–746.

infringement, whether actions, devices or software, are all material. This would certainly include contributions that (a) increase the damage caused by the infringement, (b) increase the illicit income from the infringement, (c) increase the scale of the infringement (e.g., the number of parties to whom the infringing content becomes available), or (d) provide financial or other benefit (e.g., business development benefit) from the infringement.

In EU copyright case law, there are only very limited attempts to establish contributory copyright infringement. The CJEU has attempted to stretch the rights of "communication to the public" and of "making available" to accommodate contributory copyright infringements, which would not have been needed if proper statutory regulation existed. The CJEU's attempts were based on the creative interpretation of EU Directives 2000/31/EC and 2001/29/EC, and are generally very complicated efforts to put new meaning into the economic rights of copyright under EU law, which was never conceived by the legislator. Most notable is C-527/15 *Filmspeler*, where the court held that "a communication to the public" includes when someone sells hardware with add-ons containing hyperlinks to pirate websites already installed. *Filmspeler* attempts to establish several complementary criteria for liability for infringing the right of "*a communication to the public*": "*[par 31.] The user makes an act of communication when he intervenes, in full knowledge of the consequences of his action, to give access to a protected work to his customers and does so, in particular, where, in the absence of that intervention, his customers would not, in principle, be able to enjoy the broadcast work*"

Note the "*full knowledge*" standard, which is not clarified and is much stricter than the knowledge standard in US copyright law ("*reasonable for the defendant to think that infringement was taking place*"). *Filmspeler* also required that "*protected work must be communicated using specific technical means, different from those previously used or, failing that, to a 'new public'*", and the communication to the public must be for profit ("*the profit-making nature of a communication*"). The latter conditions are endemic to digital piracy cases and for that reason not problematic, but they further complicate enforcement and would simply be unnecessary if there were proper contributory infringement rules. The latest CJEU attempt, presented in the CJEU's judgement in Cases C-682/18 *YouTube* and C-683/18 *Cyando*, is even more creative, as the court explicitly adopted the contributory infringement notion of US law, which is found nowhere else in EU statutory copyright law. The CJEU (Grand Chamber) ruled

> "1. Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain

> aspects of copyright and related rights in the information society must be interpreted as meaning that the operator of a video-sharing platform [Youtube] or a file-hosting and -sharing platform [Uploaded.to], on which users can illegally make protected content available to the public, does not make a 'communication to the public' of that content, within the meaning of that provision, unless it contributes, beyond merely making that platform available, to giving access to such content to the public in breach of copyright. That is the case, inter alia, where that operator has specific knowledge that protected content is available illegally on its platform and refrains from expeditiously deleting it or blocking access to it, or where that operator, despite the fact that it knows or ought to know, in a general sense, that users of its platform are making protected content available to the public illegally via its platform, refrains from putting in place the appropriate technological measures that can be expected from a reasonably diligent operator in its situation in order to counter credibly and effectively copyright infringements on that platform, or where that operator participates in selecting protected content illegally communicated to the public, provides tools on its platform specifically intended for the illegal sharing of such content or knowingly promotes such sharing, which may be attested by the fact that that operator has adopted a financial model that encourages users of its platform illegally to communicate protected content to the public via that platform"

Overall, these interpretations are an example of explicit judicial activism, are clearly forced, and have little to do with the right of "communication to the public" *per se*. The latter example (the joined *YouTube* and *Cyando* cases) shows undertones of influences from across the Atlantic, but, regrettably, is exceedingly specific to the "*operator of a video-sharing platform*" and "*a file-hosting and -sharing platform*", which are traditional online intermediaries. Such judicial activism and forced creativity would be unnecessary if the EU legislator would do their job of introducing proper statutory rules on contributory copyright infringement. The CJEU here did the commendable job of acknowledging the gaps in EU copyright law and laying the groundwork for contributory liability within it, but this issue has to be picked up by the EU legislator. For the rules to become effective in lower level national courts, without the need for expensive, multi-year litigation going all the way to the CJEU and back, they need to become general rules unencumbered by the specific facts and extreme conditionality of said cases.

Tort law is not part of the EU Acquis, and it would be impossible to unify the two anytime soon. Nevertheless, some aspects of torts related to intellectual property infringements (e.g. damages rules, injunctions) are already harmonised in EU Law through Directives 2000/31/EC, 2001/29/EC and 2004/48/EC, thus setting the precedent for the further *lex specialis* of intellectual property infringement torts.

There is an obvious need to harmonise contributory infringement criteria and rules. As the reasoning for this is thoroughly presented in an existing body of legal research,[22] there is no need to repeat it here. For the purposes of this article, it is most important to emphasise that harmonisation is also important because: new emerging models of digital piracy do not rely on traditional internet intermediaries and cannot be addressed through existing intermediary rules, even after the DSA updates; and digital piracy is inherently multinational (as will be illustrated by the Mobdro case study, below), spanning multiple EU jurisdictions and therefore being incapable of reasonably being addressed through national law. The reviewed US rules are not incompatible with the basic civil liability principles in European countries; therefore, the US rules may serve as the starting point for the harmonisation effort in EU copyright law, especially after the CJEU led with the surprise introduction of evidently US-influenced contributory copyright infringement terminology into substantive EU copyright law in C-682/18 *YouTube* and C-683/18 *Cyando*. The need for urgent harmonisation is further illustrated by the analysis below.

3. THE EVOLUTION OF DIGITAL PIRACY

Despite notable decreases, digital piracy remains significant and costs billions of euros per year for the EU economy.[23] Digital piracy is a dynamic phenomenon which is evolving and adapting in response to new internet technologies and internet use trends, as well as in response to legal developments. Copyright piracy is now being described as almost exclusively digital. The last two decades have seen the rapid growth of data transmission speeds, especially over wireless networks, which have

[22] Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press, pp. 42–46, Dinwoodie, G., Dreyfuss, R., and Kur, A. (2009) The Law Applicable to Secondary Liability in Intellectual Property Cases. *New York University Journal of International Law and Politics*, 2, pp. 201–235. Available from: `https://nyujilp.org/wp-content/uploads/2013/02/42.1-Dinwoodie-Dreyfuss-Kur.pdf`, Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, Available from: `https://doi.org/10.1093/jiplp/jpt213`, Angelopoulos, C. (2016) *European Intermediary Liability in Copyright: A Tort-Based Analysis*. Wolters Kluwer.

[23] EUIPO. (2021) *Online Copyright Infringement in the European Union: Music, Films and TV (2017–2020), Trends and Drivers* [online].

resulted in digital piracy shifting from P2P downloads (download now, consume later) to the streaming of digital content (download and consume simultaneously). Over the last decade, streaming piracy has far outpaced the more traditional P2P download, and, according to the latest estimates, the piracy of live TV/sports programming is more than double that of film and music piracy combined.[24] The deployment of 4G and 5G networks and global entertainment and sports phenomena also led to the surge in demand for the streaming of live entertainment and sports programming.

In 2019, it was reported that digital video piracy costs to the US economy were $29.2 billion[25] a year, while "*collective revenues, according to most estimates, have reached nine or 10 figures*".[26] Streaming piracy via unlicensed IPTV services and apps is the largest-growing section of these figures. These services represent a good market fit for consumers, who are already accustomed to online streaming as a primary form of daily entertainment. For live sports and original shows, this is also the preferred form, as nobody wants to wait until content has become stale and outdated.

The online presence during the COVID-19 pandemic led to an increased array of high-quality streaming devices and a variety of illicit content offers.[27] Live sports were especially affected by streaming piracy during the COVID-19 pandemic: a 2021 estimate of sports streaming piracy alone put damages at an estimated $28.3 billion per year.[28] While these estimates are based on the US, estimates for the EU are likely even higher due to generally higher levels of piracy (45.72% in Europe compared to 13.48% in North America in 2020[29]) and larger population numbers (almost 500 million people in the EU compared to 330 million in the US).

---

[24] *Ibid*, pp. 15–55.

[25] Blackburn, D., Eisenach, J. A., and Harrison Jr., D. (2019) *Impacts of Digital Piracy on the U.S. Economy* [online]. NERA Economic Consulting, The Global Innovation Policy Center, U.S. Chamber of Commerce. Available from: `https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf`

[26] Bushnell, H. (2019) *Inside the complex world of illegal sports streaming*. [online] Yahoo Sports. Available from: `https://sports.yahoo.com/inside-the-complex-world-of-illegal-sports-streaming-040816430.html` [Accessed 28 November 2022].

[27] EUIPO and Europol. (2022) *Intellectual Property Crime Threat Assessment 2022*. Luxembourg: Publications Office of the European Union. Available from: `https://www.europol.europa.eu/cms/sites/default/files/documents/Report.\%20Intellectual\%20property\%20crime\%20threat\%20assessment\%202022\_2.pdf` [Accessed 28 November 2022].

[28] Balderston, M. (2021) *Sports Piracy Costs $28.3B Per Year, Report Shows*. [online] TV Tech. Available from: `https://www.tvtechnology.com/news/sports-piracy-costs-dollar283b-per-year-report-shows` [Accessed 28 November 2022].

[29] Go-Globe. *Online Piracy in Numbers – Facts And Statistics* [Infographic]. [online]. Available from: `https://www.go-globe.com/online-piracy-in-numbers-facts-and-statistics-infographic/` [Accessed 3 July 2023]

The legislative effort with respect to stronger online intermediary liability rules and obligations has also caused another notable trend. Although its scope is not fully estimated, streaming piracy has increasingly taken place not on mainstream audio-visual content streaming platforms such as YouTube or Twitch, but on dedicated pirate-run digital piracy platforms. Dedicated piracy platforms are a little-researched part of the dark web, whose content is not readily accessible, not indexed by web search engines, and requires specific software, configurations, and/or authorisation to access. The main purpose of dedicated piracy platforms is to distribute pirated digital content; however, they may have multiple other purposes – e.g., to collect revenue, provide embedded services, corrupt user devices for cybercrime purposes, etc.

This trend is well illustrated by the Mobdro platform, which is analysed further in this article. At its peak in 2021, Mobdro reached an unparalleled scale of more than 100 million users. The emergence of dedicated piracy platforms implies that pirates have become adept at overcoming online intermediary-level measures aimed to contain piracy, such as filtering and blocking. For example, domain or IP address blocking is effective against websites, but not against dedicated pirate software and mobile apps, which bypass the DNS servers of online intermediaries and may use CDNs and dynamic IP addresses for the online part of their services. Moreover, digital content piracy platforms have become gateways for other criminal activities. Europol has linked piracy apps to cybercrime activities such as crypto-jacking or the distribution of malware. Pirates exploit new technologies to conceal digital traces and use proxy services to create resilient hosting networks.[30]

In a complex environment like the modern internet network, all kinds of internet infrastructure have been taken advantage of by digital pirates. From a purely instrumental perspective, it may appear that digital piracy is enabled not only by the actions of primary perpetrators, but also by the various internet platforms and services which host or distribute pirated content and run, make accessible or enable pirate services. This has been the rationale for establishing safe-harbour exceptions from secondary liability for online intermediaries, as long as they act as *bona fide* infrastructure service providers and are not aware of infringement. Internet services and internet infrastructure platforms have predominantly legitimate uses, which are not related to piracy. As a general rule, based on the so-called

[30] Turcotte, J. (2021) *Disrupting Attacker Value Propositions in Residential Networks*. [online] Doctoral dissertation, Worcester Polytechnic Institute. Available from: `https://digital.wpi.edu/downloads/1r66j4181` [Accessed 28 November 2022], EUIPO and Europol (2022).

mere conduit principle such services and platforms are considered internet intermediaries, providers of transparent services and not content controllers. Therefore, online intermediaries have been allowed safe harbour rules – a set of conditions under which intermediary service providers are exempted from liability for third party content. Safe harbour rules have been upheld multiple times in the case law; however, courts in the US and the EU have been slowly moving in the direction of limiting them in case of ignorance or sometimes even collaboration in unlawful activity by intermediaries. In US copyright law, this is underscored by the evolution from *Sony* to the *Aimster, Morpheus, Kazaa* and eventually *Grokster* cases; in EU copyright law, it is evident in the *Filmspeler*, *YouTube* and *Cyando* cases analysed in the preceding section of this article. While basic safe harbour liability exceptions are retained, the current rules include an extensive set of legal obligations with respect to protections against unlawful content (including pirated intellectual property content) extending to automatic filtering of explicitly infringing content, as well as promptly reacting to reports on infringing content. It is too early to assess the full effects of the latest rules introduced by the DSA, but it is very clear that they will have a very limited effect on the newest and currently dominant form of digital piracy: streaming piracy on dedicated platforms, such as Mobdro, which will be analysed in detail below.

As was noted, streaming piracy has been evolving towards major independent platforms dedicated to piracy which do not rely on safe harbour liability exceptions and which pretend to be legitimate only at end-user level (mainly by copying the high-quality UI and UX of legitimate platforms such as Netflix). After the OG online piracy websites such as the Pirate Bay became much more difficult to access due to blocking efforts, the opportunity emerged for blocking circumvention and piracy-concealing services, such as VPNs employed by more technically adept users, as well as for stand-alone software applications that work straight out of the box without any technical knowledge needed on part of the user.[31] This click-and-play format proved popular, with software such as Popcorn Time, Showbox and Terrarium TV attracting millions of viewers. One of the most popular click-and-play tools to emerge was Mobdro, an Android-based software application focusing on TV content from around the world. Live TV, sports channels and 24/7 content were all available on Mobdro, providing an easy-to-use solution for anyone capable of installing and running it.[32] Stand-alone software applications that

[31] Maxwell, A. (2021) *Pirate TV Streaming App Mobdro Disappears, Users in Mourning*. [online] Torrent Freak. Available from: `https://torrentfreak.com/pirate-tv-streaming-app-mobdro-disappears-users-in-mourning-210215/` [Accessed 28 November 2022].

[32] *Ibid.*

reproduce pirated content without any technical knowledge needed on part of the user are referred to as dedicated piracy platforms in this article. As was noted, by 2021 Mobdro was one of the most popular dedicated piracy platforms on the internet.

Another evolving facet of digital piracy is its monetisation. The costs involved in running and maintaining dedicated piracy platforms are significant, and require even not-for-profit pirates to seek ways to monetise their pirate operations. Traditionally, pirates would either collect direct payments in the form of subscription fees or donations or accept ads on the platform from various ad networks. Payment providers, VPN service providers and ad networks in these situations are caught up, at least indirectly, in enabling digital piracy, yet unless they knowingly and specifically profit from it, they are considered intermediaries just like almost any web service used by the pirate operation, including basic services like Google. The key aspect here is that the ad network, VPN network or payment network, like many online intermediaries, provide a basic and universal infrastructure service (a mere conduit) which can be used by anyone, including pirates.

The role of VPN networks in facilitating digital piracy is worth a separate research inquiry that is beyond the scope of this article. There are separate efforts to limit the use of payment and ad networks by pirates through stricter AML/KYC rules, as well as advertising ethics rules. These efforts have been moderately successful in at least complicating the monetisation potential of pirate platforms, while also helping to uncover perpetrators.[33] As a result, more recently the traditional direct commercialisation of illegal content (i.e., charging for access to pirated content or collecting ad revenue) has been complemented by or has competed with a new commercialisation model based on collecting fees for embedding additional services into pirate platforms.

Embedding third-party software code into another application is not a new phenomenon. Pirated content, software and services have long served as vehicles for spreading malicious code; however, until recently there have been no known cases in which the owners of the embedded code were directly paying for the operation of the pirate platform. The third-party embedded SDK model is thus an evolution in the pirate platform "business" model. From a technical perspective, this is achieved by including

[33] Batikas, M., Claussen, J., and Peukert, C. (2017) *Follow the money: Piracy and online advertising*. 28th European Regional Conference of the International Telecommunications Society (ITS): Competition and Regulation in the Information Age, Passau, Germany, 30th July–2nd August, 2017. Available from: `https://www.econstor.eu/handle/10419/169448` [Accessed 28 November 2022].

a third-party code (SDK) into the mobile, desktop or web application of the pirates. This turns the user's device into a slave node on the embedded service owner's network, which performs tasks on command from the embedded service owner (the master node). In most cases, the node operation is latent and not clearly noticeable to the user, who has installed or run a pirate app containing the embedded service node, and the ethics and lawfulness of this practice are questionable.[34] The pirates (pirate app owners) may be paid based on the number of active online instances of such embedded SDKs which are run on end-user devices; however, other models, e.g., based on uptime, volume of data transferred, etc., are certainly possible. Network security research on the residential proxy embedded SDK model has found that such SDK providers offer app developers mobile proxy SDKs as a competitive app monetisation channel, with $50,000 per month per 1 million MAU (monthly active users).[35]

There is limited research describing the functionality of such latent nodes on user devices. One common functionality involves residential proxy network nodes or user surveillance (data gathering) nodes. Note that all of this clearly raises very serious concerns on compliance with the privacy, data protection and cybersecurity regulations, and corresponding risks to consumers (the owners of end user devices, which are enslaved as proxy nodes). However, this is not investigated in this article, which is limited to copyright law and contributory liability for copyright infringements.

A key aspect of the embedded service model is that the pirate platform effectively becomes infrastructure for the embedded service network. This is the other way around compared to traditional intermediaries, where pirates are the users of an intermediary rather than providers of the infrastructure themselves. The pirate app user network thus becomes an embedded service network, and vice versa. The value of the embedded service grows alongside the size of the network where such a service is embedded, benefiting from the well-known economic network effects described by Metcalfe's law. The embedded service owner becomes directly interested in growing the pirate platform, as it also grows the embedded service network and allows the embedded service owner to collect even higher revenue from the users of embedded service. Thus, embedded services are indispensable for pirates to be able to collect revenue on their operation, which makes both sides directly

[34] Tosun, A., De Donno, M., Dragoni, N., and Fafoutis, X. (2021) RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows. In *2021 IEEE International Conference on Consumer Electronics (ICCE)*. Las Vegas: IEEE, pp. 1–6.

[35] Mi, X., Tang, S., Li, Z., Liao, X., Qian, F., and Wang, X. (2021) Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks. In *Proceeding of ISOC Network and Distributed System Security Symposium (NDSS), 2021*.

incentivised to grow the network. The latent nature of the embedded services is two-fold: it is not obvious to the consumers whose devices are enslaved as proxy nodes, and it is not clear to the users (most often businesses) of the proxy service. Without discussing the legality and ethics of the use of embedded services, it is noteworthy that the users of embedded services (e.g., business users of a residential proxy service) are very likely unaware that the service nodes are running on top of a piracy network. Research on this topic has discovered that user devices are exposed to major security and privacy risks, are often used for malicious purposes, and are likely compromised. The behaviour of residential proxies, which supposedly voluntarily serve on the network, differs starkly from expected usage in the home.[36]

This evolution of piracy "business" models highlights the limitations of the online intermediary-focused *lex specialis* – liability rules which are designed to address the use of legitimate intermediary infrastructure by bad actors (pirates), but were never designed to deal with the use of digital piracy infrastructure for non-piracy purposes, even if the latter are legitimate. While the former clearly requires carveouts from the legal liability rules for intermediaries, which is accepted in the current regulatory regime, the latter is more akin to a legal case of collaboration between two independent parties (pirates and the embedded services party) in copyright infringement – at least in maintaining and growing infrastructure whose primary purpose is mass copyright infringement on a commercial scale.

4. THE MOBDRO CASE STUDY

The Mobdro case study is representative of the evolution of digital piracy, underscored by shifts to live streaming and commercialisation through embedded services. The Mobdro app operated at least from 2018 to March 2021, and was the leading pirate streaming platform with more than 100 million users. Mobdro allowed users to stream copyrighted content (TV shows, live sports, movies, premium music videos, etc.) on Android OS devices, and was highly praised by reviewers for the availability and quality of content, including Live TV Channels (Worldwide), Live Sport Channels, the Latest Movies & TV Shows, as well as its intuitive and friendly UI and UX.[37] For all of these reasons Mobdro was the leading dedicated streaming piracy platform, which is representative of the direction that digital piracy is evolving in and provides a real-world context to the issues of contributory

[36] Turcotte, J. (2021) *Disrupting Attacker Value Propositions in Residential Networks.* [online] Doctoral dissertation, Worcester Polytechnic Institute. Available from: `https://digital.wpi.edu/downloads/1r66j4181` [Accessed 28 November 2022].

[37] Best Streaming App Reviews. *MOBDRO review.* [online]. Available from: `https://best-streaming-app.reviews/mobdro-review/` [Accessed 28 November 2022].

liability. The analysis of the Mobdro case was selected based on its relative recency and the reasonable abundance public information about it, including information from official sources (Europol) and direct evidence suggesting that Mobdro was monetised through the embedded services model. Such a case allows for the analysis of both the current digital piracy business model and the features of embedded services as intertwined phenomena. In order to achieve a maximally broad and deep analysis of the issue, the real-world case study method is the most appropriate, and case studies that allow for the analysis of multiple phenomena are preferred methodologically.[38]

The Mobdro app was not available through the official Google Play store; however, it was distributed as an APK download in alternative app stores (e.g., APK Free or F-Droid). It was also widely distributed as preloaded software on Android IPTV sticks (such as the Amazon Fire TV stick), which were sold online through various e-commerce marketplaces.

Although the makers of the Mobdro software were anonymous, the Mobdro application had more than 100 million users, and by that measure alone could be compared in popularity to such major legitimate audio-visual digital content platforms as Disney+ or HBOMax. Moreover, the Mobdro user count well exceeded that of multiple global streaming platforms such as Twitch, Tidal, Deezer, Pandora, and Apple TV.[39] The number of users of the Mobdro app is a direct determinant of the size and scale of the pirate network, and hence directly implies the unparalleled scale of this case: Mobdro was clearly a major global player – a whale – in the content streaming marketplace by any standard.

The scale and activities of Mobdro came to light in the context of a Europol investigation, which culminated in the March 2021 takedown of the main Mobdro infrastructure. Europol received complaints from rights holders, among them main European football leagues, about a mobile application illegally distributing video streams. According to Europol, "*The application, downloaded by more than 100 million users via different websites, illegally offered the streaming of videos and TV channels. The Europol investigation identified a number of connected websites and platforms located in Spain and Portugal with connections to servers in Czech Republic*". In addition, according to Europol, the "*Spanish company behind the illegal activity earned its profits through advertisements. Through the computer infrastructure and power, they were able to sell user information to a company related to botnet and DDoS attacks. Investigators*

[38] Gerring, J. (2017) *Case Study Research: Principles and Practices*. 2nd Ed. Cambridge: Cambridge University Press, p. 37.

[39] Snigdha, B. (2022) *Top Streaming Statistics for 2022*. [online] SaaS Worthy. Available from: `https://www.saasworthy.com/blog/top-streaming-statistics/`[Accessed 28 November 2022].

estimate the overall illegal profits at more than €5 million." Note that this is only the direct profit of Mobdro, while the damage done was likely far in excess of this amount. While the Mobdro takedown terminated its infringements, it took multiple years, and it did not address the damages to rightsholders caused by Mobdro and contributors to its operations.

It is noteworthy than in its default mode the Mobdro app operated with embedded services enabled, and only if the user opted out of the embedded services (third party SDK) were they shown ads. It is unclear whether embedded SDK was dormant or operational in ad mode, and how many users actually chose to run it in ad mode. It is also possible that the Mobdro app had multiple embedded SDKs. A Europol report on Mobdro references the fact that "*Through the computer infrastructure and power, they were able to sell user information to a company related to botnet and DDoS attacks*", which suggests monetisation through embedded SDK services.

One Mobdro-embedded SDK service-provider may have been the provider of the embedded SDK focusing on residential proxy network infrastructure, which they admitted themselves when suspending the SDK available to Mobdro after Europol action.[40] This operator of a residential proxy network stated that they "*have zero tolerance to illegal activities. When it came to our attention that Mobdro (a publisher which was using our commercial SDK) had been subject to a law enforcement investigation for alleged copyright infringement, we suspended their right to use our SDK*". However, this provider did not clarify what their relationship and commercial arrangement with the Mobdro publishers was.[41] The costs of residential proxy service providers for clients are based on the number of proxies used and data transfer volume[42]; therefore, it is reasonable to assume that the relationship between Mobdro and this SDK provider was continuous – i.e., Mobdro was continuously and periodically paid to host SDK based on the MAU of the Mobdro app.

In case of residential proxy SDKs, according to cybersecurity research, such SDKs turn the Android device running the app into a peer on a residential proxy network. The device becomes a network node, where the internet address and bandwidth of the Android device are used for unknown purposes. Such networks have previously been named malicious, dark services, and have been compared to botnets by network security

[40] Maxwell, A. (2021) *Mobdro: Luminati Proxy Service "Suspended Service" To Pirate App*. [online] Torrent Freak. Available from: `https://torrentfreak.com/mobdro-luminati-proxy-service-suspended-service-to-pirate-app-210315/` [Accessed 28 November 2022].

[41] *Ibid*.

[42] Proxy Way. (2023) *10 Best Residential Proxies of 2023*. [online]. Available from: `https://proxyway.com/best/residential-proxies`

researchers.[43] However, the full details of the Mobdro embedded service network are yet to be established.

The Mobdro case highlights the major risks not only of copyright infringement, but also regarding privacy and personal data, as well as from cybersecurity perspectives, since, according to Europol, it involved the sale of user information and may have exposed user devices to unsolicited data transfers. Mobdro was also not a one-off host for the embedded SDK, as such embedded services appear to be the predominant model to monetise various apps, of which many are related to piracy.

5. PARTIES BEHIND EMBEDDED SERVICES: INTERMEDIARIES OR COLLABORATORS?

It may be a useful exercise to try to map the known circumstances of the Mobdro case onto the conditions of contributory copyright infringement previously summarised in this article in order to evaluate the legal status of the party behind embedded services.

There is no doubt that the Mobdro developers and publishers were the direct infringers in this case. Mobdro was also a major player in content streaming, boasting more than 100 million installs, yet the developers stayed anonymous and the app was not distributed through the official Google Play app store, which normally requires clear disclosure of the app developers and subjects the app to the Google vetting process. Despite the app running the live broadcasting of major sport leagues, no legitimate content partnerships were publicly reported or confirmed. In 2018, reputable media sources already publicly reported doubts on the lawfulness of Mobdro.[44] In addition, by 2021 Mobdro had accumulated a handful of DMCA notice and takedown complaints.[45] These circumstances certainly suggest that Mobdro was engaging in copyright infringement "business", and it was public knowledge. Mobdro partners either knew of the illegitimacy of Mobdro operations or

[43] See Mi, X. et al. (2019) Resident Evil: Understanding Residential IP Proxy as a Dark Service. In *2019 IEEE Symposium on Security and Privacy (SP)*. San Francisco: IEEE, pp. 1185–1201; Hacid, H. et al. (Eds.). (2021) *Service-Oriented Computing – ICSOC 2020 Workshops*. Spinger, Cham; Tosun, A., De Donno, M., Dragoni, N., and Fafoutis, X. (2021) RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows. In *2021 IEEE International Conference on Consumer Electronics (ICCE)*. Las Vegas: IEEE, pp. 1–6.

[44] Williams, A. (2018) *Mobdro: the app that wants to take on Kodi for a shot at the streaming crown*. [online] Tech Radar. Available from: `https://www.techradar.com/news/mobdro-the-app-that-wants-to-take-on-kodi-for-a-shot-at-the-streaming-crown` [Accessed 28 November 2022].

[45] Maxwell, A. (2021) *Pirate TV Streaming App Mobdro Disappears, Users in Mourning*. [online] Torrent Freak. Available from: `https://torrentfreak.com/pirate-tv-streaming-app-mobdro-disappears-users-in-mourning-210215/` [Accessed 28 November 2022].

had multiple direct and serious reasons to know and doubt the legitimacy thereof. It is implausible that the SDK developer did not have knowledge of the activities performed by the app where their SDK was embedded, especially since the relationship between Mobdro and the SDK providers was continuous, and the network of nodes supplied by Mobdro was very sizable (if not the largest). Separately, it is noteworthy that the residential proxy business which is known to rely on embedded service SDKs is highly lucrative and generates hundreds of millions dollars in revenue[46]; therefore, entities engaged in this business have ample resources with which to do due diligence on the platforms which run their residential proxy SDKs. Failure to know the customer (or business partner, as in the case between Mobdro and its SDK provider) at the very least raises serious questions about the fulfilment of duties of care, and may allow applications of vicarious liability, but this analysis would go beyond the scope of this article.

Collaboration between Mobdro and the providers of the embedded services SDK had to be significant, since at minimum such collaboration would include software code exchange, payment, as well as some form of accounting of MAU, on which the payment would be based. All of these cooperation activities are continuous and periodical (likely monthly). A significant and continuous relationship is necessitated by multiple distinct reasons. First, the MAU accounting and payments by the SDK provider for the services of the Mobdro platform. Second, the technical integration of the SDK and the Mobdro app. Both the SDK and the app underwent multiple versions (software updates) over the years,[47] and continuous technical functioning of the two would be impossible if there were not continuous technical collaboration and exchange of updates between the two parties. Since the SDK is part of the software code of the pirated app, the maker of such an SDK would normally provide support and maintenance with respect to integrating the SDK, and would maintain it up to date in subsequent releases of the new versions of the pirate app. Based on the basic analysis of versions of the Mobdro app available in the Internet Archive,[48] the software code of the embedded SDKs was obfuscated, at the very least to hide it from competition and deter reverse engineering, which further underscores the notion of continuous collaboration. Code obfuscation during compilation is

[46] Maayan, M. (2021) *Bright Data CEO: "We have crossed $100 million in annual revenue"*. [online] CTech, 12 December. Available from: `https://www.calcalistech.com/ctech/articles/0,7340,L-3924814,00.html` [Accessed 28 November 2022].

[47] Archive images of the Mobdro website suggest more than a dozen releases and multiple versions of the Mobdro app. See: `https://web.archive.org/web/20200810194730/https://mobdro.org/` [Accessed 3 July 2022]

[48] *Ibid*.

normally achieved by close cooperation between the provider of the code and the party compiling the final application, so that the functionality of the SDK is not impaired. All of this evidence of a continuous relationship between Mobdro and the SDK provider is a very important aspect from which to establish the collaborative and contributory nature of the relationship between the two. In turn, this can establish the causal and contributory relationship of the SDK in the copyright infringing activities of the piracy platform.

As was already noted, for the embedded service providers the Mobdro network is an important part of service infrastructure. The provider of the embedded services SDK has a vested interest in the growth of the Mobdro user base, since it also grows the embedded services infrastructure. This in turn would grow the income from the Mobdro operation for both parties and increase the scale of the infringement (the number of Mobdro end users). Thus, it is reasonable to assume, and it would not be surprising if it were the case, that the growth of the Mobdro user base (e.g., Mobdro marketing) was incentivised through payments by the SDK. However, even if it was not actively incentivised by the SDK provider, it is clear that Mobdro growth financially benefitted both Mobdro and the SDK provider, and thus the SDK provider directly (through the growth of the Mobdro network) benefitted from copyright infringement committed by Mobdro, as it would grow the business of the SDK provider.

In addition to the SDK provider's contribution to the relationship between themselves and Mobdro, it is independently useful to note that each actual act of piracy on the Mobdro platform (i.e., a Mobdro user running the Mobdro app and watching pirated content streamed by Mobdro) was an active node for the SDK provider. Thus, the SDK provider was actually directly benefiting from each act of copyright infringement committed by Mobdro.

All of this suggests material, indirect contribution to the Mobdro operation by the embedded service provider; their intentional participation in and benefit from the actual operation of the Mobdro app; and the implausibility of the idea that the SDK provider had no knowledge of the Mobdro "business" of copyright infringement, or had no intent with respect to Mobdro continuing and expanding their operations. In the studied case, all activities of the Mobdro app in the EU were *prima facie* illegitimate from a copyright law perspective, and there was not even a single attempt to portray them as legitimate. As was noted, serious legitimacy concerns were raised very early into Mobdro's operations, even by non-legal reviewers. In such a situation, the SDK provider could not have expected any legitimate use of the Mobdro platform, and no explanation to that end was provided

by the SDK provider in the post-takedown acknowledgment.[49] Instead, the SDK provider only denied their awareness of Mobdro's illegitimacy, which was already rebutted by the arguments above. The SDK provider had every reason to be aware of Mobdro's activities, and at the very least failed to perform due diligence where it would have been mandatory.

The assumptions in this mapping exercise are based on public information, which is not necessarily vetted and supported by evidence admissible in a court of law, yet this activity demonstrates that the contributory liability criteria appear to have been met in multiple ways. If the operations of the Mobdro platform and the SDK provider would have taken place in the US, the SDK provider would be in serious risk of facing contributory liability for copyright infringement. In the EU, where statutory contributory infringement rules are not available, the SDK provider continues without charge. If contributory liability for copyright infringement rules were available, it is likely that Mobdro would have been shut down much faster through civil action, and there would be opportunities for rightsholders to seek recovery of damages from the contributor – the SDK provider.

The takedown of Mobdro has immediately led to the appearance of multiple copycat streaming piracy platforms attempting to imitate Mobdro. So far, no party has been reported to be facing legal liability for the copyright infringements of the Mobdro pirate platform. The lack of cross-border statutory rules for contributory infringement in the EU is certainly not helpful in this case.

6. CONCLUSION

The lack of contributory liability rules represents a significant gap in substantive EU copyright law, which puts EU rights holders at a disadvantage compared to US rights holders. In the US, copyright case law has adopted a contributory liability doctrine and developed reasonable conditions to enforce such liability against parties contributing to copyright infringement independently from tort law remedies.

This gap is recognised in the jurisprudence, which has advocated for the harmonisation of the EU rules on this matter for more than a decade. In few EU countries, this gap is conditionally filled though national case law by the creative application of national tort law doctrines. The CJEU attempted – in C-527/15 *Filmspeler*, and more recently in joined cases C-682/18 *YouTube* and

[49] Maxwell, A. (2021) *Mobdro: Luminati Proxy Service "Suspended Service" To Pirate App*. [online] Torrent Freak. Available from: `https://torrentfreak.com/mobdro-luminati-proxy-service-suspended-service-to-pirate-app-210315/` [Accessed 28 November 2022]

C-683/18 *Cyando* – to fill this gap with commendable judicial activism based on the stretched interpretation of the "right to communicate to the public", and even the explicit introduction of contributory copyright infringement terminology into substantive EU substantive copyright law. Nevertheless, neither the tort law approach nor the latest CJEU approach are practical against the modern actors of digital piracy, as is evidenced by the very limited enforcement of copyright against parties that contribute to digital piracy in the EU and the continuous, multi-year operations of modern digital piracy platforms such as Mobdro within its borders. This is an acute problem which was nevertheless left out of the EU Digital Services Act (DSA), which only updated the online intermediary liability rules in EU law.

Neither the expansion of the right to communication to the public, nor national tort law, nor the rules governing online intermediary liability are equipped to address rapidly evolving and multinational digital piracy. Digital pirates have demonstrated adaptability to enforcement at the intermediary level by migrating to dedicated digital piracy platforms, which generate significant revenue through embedded services. The providers of these embedded services, not being online intermediaries, exploit this legal quagmire, utilising piracy infrastructure as an integral part of their services and thereby contributing to digital piracy. The case study of Mobdro presented in this article highlights the multinational reach and vast scope of these new digital piracy platforms, which surpass even their legitimate digital content counterparts. While Mobdro has been dismantled, this was the result of a lengthy effort for which final legal resolution remains pending. In the interim, dozens of new digital piracy platforms, monetised through embedded services, persist. Due to the absence of contributory liability rules, it is also problematic for rightsholders to seek civil damages relief from the parties that contributed to Mobdro's operations and profited from them. Separately, the Mobdro case study further illustrates how digital piracy is entwined with data protection and cybersecurity risks. These aspects, although not covered in this article, undoubtedly warrant separate legal research inquiries.

Judicial activism and forced judicial creativity would be unnecessary if the EU legislator would do their job of introducing proper statutory rules on contributory copyright infringement. In said judgements, the CJEU underscored this need and laid the groundwork for contributory liability in EU copyright law, but the job needs to be finished by the EU legislator. The simplest way that embedded services-fuelled piracy can be addressed is via the introduction of general statutory rules on contributory infringement. The limited statutory precedent of harmonising intellectual property tort

rules already exists in EU law. These rules should be modelled on US law, as was largely accomplished with online intermediary liability rules. By codifying them into statutory copyright law, the EU would reign in threats of digital piracy, enhance regulatory certainty and minimise national distortions. The conditions are ripe for such an effort at the EU level, and the proposed revision of the 2004/48/EC Enforcement Directive[50] may present an opportunity to address this matter.

LIST OF REFERENCES

[1] Angelopoulos, C. (2016) *European Intermediary Liability in Copyright: A Tort-Based Analysis*. Wolters Kluwer.

[2] Balderston, M. (2021) *Sports Piracy Costs $28.3B Per Year, Report Shows*. [online] TV Tech. Available from: https://www.tvtechnology.com/news/sports-piracy-costs-dollar283b-per-year-report-shows [Accessed 28 November 2022].

[3] Bartholomew, M., and McArdle, P. F. (2011) Causing infringement. Vanderbilt Law Review, 64 (3), pp. 675–746.

[4] Batikas, M., Claussen, J., & Peukert, C. (2017) *Follow the money: Piracy and online advertising*. 28th European Regional Conference of the International Telecommunications Society (ITS): Competition and Regulation in the Information Age, Passau, Germany, 30th July–2nd August, 2017. Available from: https://www.econstor.eu/handle/10419/169448 [Accessed 28 November 2022].

[5] Best Streaming App Reviews. *MOBDRO review*. [online]. Available from: https://best-streaming-app.reviews/mobdro-review/ [Accessed 28 November 2022].

[6] Blackburn, D., Eisenach, J. A., and Harrison Jr., D. (2019) *Impacts of Digital Piracy on the U.S. Economy* [online]. NERA Economic Consulting, The Global Innovation Policy Center, U.S. Chamber of Commerce. Available from: https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf

[7] Bushnell, H. (2019) *Inside the complex world of illegal sports streaming*. [online] Yahoo Sports. Available from: https://sports.yahoo.com/inside-the-complex-world-of-illegal-sports-streaming-040816430.html [Accessed 28 November 2022].

[50] European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Peter, V., Radauer, A., Markianidou, P., et al. (2017) *Support study for the ex-post evaluation and ex-ante impact analysis of the IPR enforcement Directive (IPRED): final report*. Luxembourg: Publications Office of the European Union, doi:10.2873/903149.

[8] Davis Powell, C. (2009) The Saga Continues: Secondary Liability for Copyright Infringement Theory, Practice and Predictions. *Akron Intellectual Property Journal*, 3 (1), Article 7. Available from: https://ideaexchange.uakron.edu/akronintellectualproperty/vol3/iss1/7

[9] Dinwoodie, G., Dreyfuss, R., and Kur, A. (2009) The Law Applicable to Secondary Liability in Intellectual Property Cases. *New York University Journal of International Law and Politics*, 2, pp. 201–235. Available from: https://nyujilp.org/wp-content/uploads/2013/02/42.1-Dinwoodie-Dreyfuss-Kur.pdf

[10] EUIPO. (2021) *Online Copyright Infringement in the European Union: Music, Films and TV (2017–2020), Trends and Drivers* [online]. DOI:102814/505158.

[11] EUIPO and Europol. (2022) *Intellectual Property Crime Threat Assessment 2022*. Luxembourg: Publications Office of the European Union. Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/Report.\%20Intellectual\%20property\%20crime\%20threat\%20assessment\%202022_2.pdf [Accessed 28 November 2022].

[12] European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Peter, V., Radauer, A., Markianidou, P., et al. (2017) *Support study for the ex-post evaluation and ex-ante impact analysis of the IPR enforcement Directive (IPRED): final report*. Luxembourg: Publications Office of the European Union.

[13] Folsom, T.C. (2009) Toward Non-Neutral Principles of Private Law: Designing Secondary Liability Rules for New Technological Uses. *Akron Intellectual Property Journal*, 3, pp. 43-104.

[14] Frosio, G. (ed.) (2020) *Oxford Handbook of Online Intermediary Liability*. OUP.

[15] Gerring, J. (2017) *Case Study Research: Principles and Practices*. 2nd Ed. Cambridge: Cambridge University Press.

[16] Go-Globe. *Online Piracy in Numbers – Facts And Statistics* [Infographic]. [online]. Available from: https://www.go-globe.com/online-piracy-in-numbers-facts-and-statistics-infographic/ [Accessed 3 July 2023]

[17] Hacid, H. et al. (Eds.). (2021) *Service-Oriented Computing – ICSOC 2020 Workshops*. Spinger, Cham, doi:10.1007/978-3-030-76352-7.

[18] Husovec, M. (2013) Injunctions against Innocent Third Parties: The case of Website Blocking. *JIPITEC*, 4, pp. 116–129.

[19] Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press.

[20] Kravets, D. (2009) *English Transcript of Pirate Bay Guilty Verdicts Released*. [online] Wired. Available from: https://www.wired.com/2009/04/english-transcript-of-pirate-bay-guilty-verdicts-released/

[21] Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, https://doi.org/10.1093/jiplp/jpt213

[22] Lemley, M. A., and Reese, R. A. (2004) Reducing Digital Copyright Infringement Without Restricting Innovation. Stanford Law Review, 56 (6), pp. 1345–1434.

[23] Maayan, M. (2021) *Bright Data CEO: "We have crossed $100 million in annual revenue"*. [online] CTech, 12 December. Available from: https://www.calcalistech.com/ctech/articles/0,7340,L-3924814,00.html [Accessed 28 November 2022].

[24] Maxwell, A. (2021) *Mobdro: Luminati Proxy Service "Suspended Service" To Pirate App*. [online] Torrent Freak. Available from: https://torrentfreak.com/mobdro-luminati-proxy-service-suspended-service-to-pirate-app-210315/ [Accessed 28 November 2022].

[25] Maxwell, A. (2021) *Pirate TV Streaming App Mobdro Disappears, Users in Mourning*. [online] Torrent Freak. Available from: https://torrentfreak.com/pirate-tv-streaming-app-mobdro-disappears-users-in-mourning-210215/ [Accessed 28 November 2022].

[26] Mehra, S.K. (2011) Keep America Exceptional! Against Adopting Japanese and European-Style Criminalization of Contributory Copyright Infringement. *Vanderbilt Journal of Entertainment and Technology Law*, 13 (4).

[27] Mi, X. et al. (2019) Resident Evil: Understanding Residential IP Proxy as a Dark Service. In *2019 IEEE Symposium on Security and Privacy (SP)*. San Francisco: IEEE, pp. 1185–1201.

[28] Mi, X., Tang, S., Li, Z., Liao, X., Qian, F., and Wang, X. (2021) Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks. In *Proceeding of ISOC Network and Distributed System Security Symposium (NDSS), 2021*. DOI: 10.14722/ndss.2021.24008.

[29] Ninth Circuit Jury Instructions Committee (2017) 17.21. Derivative Liability—Contributory Infringement—Elements and Burden of Proof. In: Manual of Model Civil Jury Instructions [online]. Available from: https://www.ce9.uscourts.gov/jury-instructions/node/279 [Accessed 28 November 2022].

[30] Proxy Way. (2023) *10 Best Residential Proxies of 2023*. [online]. Available from: https://proxyway.com/best/residential-proxies

[31] Snigdha, B. (2022) Top Streaming Statistics for 2022. [online] SaaS Worthy. Available from: https://www.saasworthy.com/blog/top-streaming-statistics/[Accessed 28 November 2022].

[32] Tilly, J. M. (2008) Perfect 10 v. Visa: the future of contributory copyright infringement. *Oklahoma Law Review*, 61 (4), pp. 865–890.

[33] Tosun, A., De Donno, M., Dragoni, N., and Fafoutis, X. (2021) RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows. In *2021 IEEE International Conference on Consumer Electronics (ICCE)*. Las Vegas: IEEE, pp. 1–6.

[34] Turcotte, J. (2021) *Disrupting Attacker Value Propositions in Residential Networks*. [online] Doctoral dissertation, Worcester Polytechnic Institute. Available from: https://digital.wpi.edu/downloads/1r66j4181 [Accessed 28 November 2022].

[35] Williams, A. (2018) *Mobdro: the app that wants to take on Kodi for a shot at the streaming crown*. [online] Tech Radar. Available from: https://www.techradar.com/news/mobdro-the-app-that-wants-to-take-on-kodi-for-a-shot-at-the-streaming-crown [Accessed 28 November 2022].