E

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

WIPO/ACE/17/13
ORIGINAL: ENGLISH
DATE: DECEMBER 31, 2024

Advisory Committee on Enforcement

Seventeenth Session
Geneva, February 4 to 6, 2025

STUDY ON THE EFFECTIVENESS AND THE LEGAL AND TECHNICAL MEANS OF IMPLEMENTING WEBSITE-BLOCKING ORDERS*

*prepared by Mrs. Maria Fredenslund, Attorney-at-law and Director at the Danish Rights Alliance (RettighedsAlliancen), Mr. Graziano Giannini, PhD and Advisor at the Italian Communications Regulatory Authority (AGCOM) and Mr. Dean Marks, Attorney-at-law and Emeritus Director of the Coalition for Online Accountability***

ABSTRACT

The blocking of piracy websites by Internet service providers is becoming one of the most widely adopted remedies for online copyright piracy. Blocking websites has proven effective in preventing Internet users from accessing illegal websites and in encouraging increased use of legal sites and servicesfor enjoying copyrighted content. The study examines the effectiveness of website-blocking orders (or site-blocking orders) and how they are implemented, the legal basis for blocking websites and how it has become an efficient means of reducing traffic to sites and services that infringe copyright.

* This study was undertaken with the support of the Ministry of Culture, Sports and Tourism of the Republic of Korea.
** The views expressed in this document are those of the authors and not necessarily those of the Secretariat or of the Member States of WIPO. Special thanks go to Jorge Alberto Bacaloni, Regional Anti-Piracy Manager at DIRECTV Latin America, for his insightful contributions to this study.
*** All Internet sources were last accessed on December 12, 2024.

Website blocking is controversial in some countries and has become routine in others. The study examines what makes a blocking system effective and provides practical guidance on obtaining and implementing blocking orders in various jurisdictions.

It also explores legal and technical developments to maintain the effectiveness of blockings. It also sets forth recommendations for forward-looking blocking policies and technical implementations based on the premise that a blocking system must be dynamic rather than static in order to keep pace with current technologies and innovation.

I. INTRODUCTION AND SCOPE

1. Online copyright infringement at a commercial scale, often referred to as copyright piracy, poses significant challenges. Digital technology makes it relatively easy to copy and make available copyrighted content online without the authorization of the rights owner. According to one study, piracy sites around the globe received more than 219 billion visits in 2022.[1]

2. The motivation for criminals to infringe intellectual property rights (IPRs) instead of committing "traditional" crimes is high, mainly because:

- Content, such as television programs and music, is easy to acquire and easy to distribute online without authorization;
- Users are attracted to websites and online services offering "free" films, music, video games or live sports;
- Return on investment is high, based on advertising revenues, subscriptions and/or engagement in the "dark web"[2]; and
- The risk of the websites being closed down is low as is the risk of the operators being caught and prosecuted for criminal copyright infringement. Moreover, even if the operators are caught and successfully prosecuted, criminal sentences for IP crimes tend to be relatively light (see, for example, the case of The Pirate Bay, described in annex 1).

3. Users of piracy websites and online services are driven by the easy access to popular content and products, which seem to be free or very inexpensive. However, they expose themselves to the threat of being in the hands of infringers who do not comply with principles of data safety or other legal rules and often use the traffic to commit other types of crime, such as stealing personal information, installing malware, using ransomware or conducting hacking attacks.[3] According to one investigation in 2022, nearly 80 per cent of piracy sites serve malware-ridden advertisements to their users.[4] Interpol reported in 2023 that "many websites and peer-to-peer networks that offer pirated material may contain malware or viruses, which can harm the user's device or steal personal information. This malware can also spread in parallel

---

1 Muso Discover, "Unlicensed Demand Report", August 2023, chrome-https://www.wipo.int/documents/1697652/2826959/muso-wipo-alert-report-march-2023.pdf/147d0f61-ba0e-bfe0-6c08-2e848b3f1c4e?version=1.1&t=1707729561252.

2 Digital Citizens Alliance, "Fishing in the Piracy Stream: How the Dark Web of Entertainment is Exposing Consumers to Harm", April 2019.

3 Internet Matters, "Internet safety and the dangers of digital piracy: Understanding the risk for children", July 2018; and Digital Citizens Alliance, "Fishing in the Piracy Stream: How the Dark Web of Entertainment is Exposing Consumers to Harm", April 2019.

4 Fadilpasic, Sead, "Piracy sites are bombarding users with malicious ads to download actual malware", Techradar, September 2022, https://www.techradar.com/news/piracy-sites-are-bombarding-users-with-malicious-ads-to-download-actual-malware.

within a home or corporate network, potentially affecting critical business operations, or be used as the launchpad for identity theft and identity fraud."[5]

4. Apart from the dangers to users, numerous studies have concluded that "digital piracy harms creators by reducing their ability to make money from their creative efforts" and "harms society by reducing the economic incentives for investment in creative output".[6] A study by the United States Chamber of Commerce found that online piracy costs the US economy at least $29.2 billion in lost revenue and more than 230,000 jobs a year.[7] The High Court of Delhi, in India, observed: "It is important to realize that piracy reduces jobs, exports and overall competitiveness in addition to standards of living for a nation and its citizens."[8] A study of piracy in Latin America found that online piracy alone causes a loss of tax revenues for eight Latin American countries in excess of US$1.32 billion.[9]

5. Enforcement of copyright online poses challenges because sophisticated infringers frequently operate out of foreign jurisdictions and use resources, such as hosting providers, content delivery networks and domain name service providers located in different countries. As was noted in a report in 2024, pirates "typically operate from abroad and across multiple jurisdictions … [and] the countries from which they operate often have less strict copyright laws—or they don't enforce them—making it difficult or impossible to catch the infringers and bring them to justice".[10] Even when infringers are caught and prosecuted, the copyright piracy websites they created often still spring back up and persist on other online infrastructures and services (see annex 1 for an example concerning The Pirate Bay website).

6. Given the jurisdictional challenges posed by online copyright piracy and the resilience of many piracy operators and websites, alternative remedies have become necessary. The blocking by Internet access/service providers (ISPs) of copyright infringing websites, known as site blocking, has been adopted widely. National authorities order ISPs to deny their users access to specific websites and online services engaged in copyright piracy. When a user of an ISP subject to a site-blocking order types the name of a piracy website covered by the order into their web browser, then instead of being taken to the website the user receives an error message or a message stating that the website concerned engages in illegal activity and therefore has been blocked.[11]

7. The power of national courts to address operators of piracy websites located beyond their jurisdiction is limited. Such limits are exacerbated by the fact that domain names can be acquired anonymously from domain name registration services around the world and that servers and website hosting providers may be located in countries with poor enforcement. That makes it easy for operators of piracy websites to avoid civil actions and criminal prosecution by operating abroad and using services across multiple countries to escape enforcement authorities. National courts do, however, have the jurisdiction and ability to impose orders on

---

5 Interpol, "Digital Piracy", https://www.interpol.int/en/Crimes/Illicit-goods/Shop-safely/Digital-piracy.

6 Smith, Michael D., "What the Online Piracy Data Tells Us About Copyright Policymaking", Hudson Institute, April 2023, https://www.hudson.org/intellectual-property/what-online-piracy-data-tells-us-about-copyright-policymaking.

7 US Chamber of Commerce, "Impacts of Digital Piracy on the US Economy," June 2019, https://www.uschamber.com/technology/data-privacy/impacts-of-digital-piracy-on-the-u-s-economy.

8 *UTV Software Communication Ltd. and others v. 1337X.To and others*, High Court of Delhi at New Delhi, April 10, 2019 (para. 29), https://indiankanoon.org/doc/47479491/.

9 Alianza 2024 Report, https://urldefense.com/v3/__https:/alianzaaudiovisual.net/admin/uploaded_files/recurso_file_d08f3ab914248d9b5caa65a9e5fa9235.pdf__;!!ChWRnQ646yhd!QLu9xFME1XTJJ_CeDxhcKx9-cBrAu-cVHm3uwMpeDiKa1uSl_6PtmY2QH2zuG9S0Y-H5rxUhLQwWuJdEDLk$.

10 IP House, "Overseas and Out of Reach", September 2024, https://reports.digitalcitizensalliance.org/ip-house.

11 Site blocking has been applied not only in relation to copyright infringing websites, but also to websites engaged in the sale of unsafe products, distribution of child sexual abuse material, unauthorized gambling and other illegal activities.

ISPs providing access to the Internet to the residents of their countries. National authorities can embrace site blocking to reduce access to piracy websites that exist and operate beyond their jurisdiction. Site blocking does not remove such websites from the Internet, but it does keep users from accessing them, consuming the infringing content offered on them and exposing themselves to potential harm, such as through identity theft and malware. Site blocking operates on a country-by-country basis. Thus, a site-blocking order in a country with respect to a particular copyright-infringing website or online service applies only to ISPs and Internet users in that country. As one scholar has noted, "the underlining premise is simple: by making it harder to access illegal content, government can encourage more people to use legal content services and thus support actual content creators—and not the piracy operators who want to profit off their hard work".[12] To date, more than 50 countries around the world, including those with robust economies and those with developing economies, have adopted site blocking.[13]

IMAGE 13: Site-Blocking is Used in Over 50 Countries Around the World.

8. While no single remedy or "silver bullet" exists to prevent or completely disable online copyright piracy, site blocking has proven effective in reducing revenue flows to criminals and preventing Internet users from accessing illegal and unsafe websites. According to the Information Technology and Innovation Foundation, "website blocking for copyright infringement has been normalized as a tool to fight digital piracy and support legal content creators and services, whether it's TV, film, books, video games, or music".[14]

9. This study focuses on the following aspects of site blocking:

(a) The effectiveness of site blocking in terms of reducing access to copyright piracy sites and services and increasing the consumption of copyrighted content from legal sources.

(b) The legal basis in various countries around the world for imposing site-blocking orders and the legal processes for obtaining them.

---

12 Corey, Nigel, "Website Blocking in Europe: Debated, Tested, Proved and Defended", Information Technology & Innovation Foundation, May 2021, https://itif.org/publications/2021/05/07/website-blocking-europe-debated-tested-approved-and-defended/.

13 IP House, "Overseas and Out of Reach", September 2024, https://reports.digitalcitizensalliance.org/ip-house.

14 Corey, Nigel, "A Decade After SOPA/PIPA, It's Time to Revisit Website Blocking", Information Technology & Innovation Foundation, January 2022, https://itif.org/publications/2022/01/26/decade-after-sopa-pipa-time-to-revisit-website-blocking/.

(c) The technical aspects of implementing site-blocking orders, including the related burdens and costs, and the technical means of circumventing such orders.

(d) How courts around the world have addressed concerns that site blocking may conflict with fundamental rights, such as free speech and privacy.

(e) A practical analysis of future challenges for site-blocking orders and mechanisms that can help to preserve their effectiveness.

II. EFFECTIVENESS OF SITE BLOCKING

10. Site blocking has been used to combat online copyright piracy for almost 20 years.[15] Around the world, site-blocking orders issued by courts and administrative agencies have disabled user access to more than 90,000 domain names used by over 27,000 piracy websites.[16] Across various countries and regions, studies have consistently demonstrated that site blocking, when applied to a significant number of such websites, helps to reduce the volume of visits to them and encourage greater use of legal services to consume copyrighted content.

11. A recent study of site-blocking orders in Brazil and India found that site blocking is "an effective tool to reduce piracy and increase legal consumption".[17] In Brazil, the study found that site-blocking orders applied since 2021 to 174 piracy websites had resulted in a 5.2 per cent increase in content consumption from legal services.

12. In India, the study found that site-blocking orders applied since 2019 to 380 piracy websites had resulted in an 8.1 per cent increase in content consumption from legal services. Blocking orders applied since 2020 to 173 piracy websites had resulted in an additional 3.1 per cent increase in content consumption from legal services. Internet traffic from users in Brazil and India to the websites subject to blocking orders had decreased considerably. The authors of the study concluded that the site-blocking orders issued in 2021 alone in Brazil and in 2019 and 2020 in India had led to a substantial drop in visits to the piracy websites and, more importantly, "statistically and economically significant increases in usage of legal media sites".[18]

13. In the Asia-Pacific region, a study conducted in 2023 by the Coalition Against Piracy found: "For those countries that are implementing site blocking effectively, there continue to be demonstrable effects in behavioral change, with 62 per cent of consumers in Indonesia and 64 per cent in Malaysia indicating that they have changed their viewing habits as a result of piracy sites being blocked. Both of these countries have long-running, effective and efficient regulatory blocking regimes. In Singapore, one of the first countries in the region to allow rights holders to protect their content via the provision of judicial site-blocking measures, it is notable that, after almost 10 years of the measure being in place, Singapore has the lowest percentage of consumer piracy in the region, with only 39 per cent of consumers pirating."[19]

---

15 The first injunction issued against an ISP to block access to a website trafficking in copyright-infringing content was in Denmark in 2006. *IFPI Denmark v. Tele2*, Copenhagen District Court, October 2006, Case F1 15124/2006. See also https://arstechnica.com/information-technology/2006/10/8080/.

16 IP House, "Overseas and Out of Reach", September 2024, https://reports.digitalcitizensalliance.org/ip-house.

17 Danaher, Brett; Sivan, Liron; Smith, Michael D.; Telang, Rahul, "The Impact of Online Piracy website Blocking on Legal Media Consumption", February 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4723522.

18 Ibid.

19 AVIA PR, "2023 CAP Consumer Surveys Continue to Show the Benefits of Effective Site Blocking", May 2023, https://avia.org/2023-cap-consumer-surveys-continue-to-show-the-benefits-of-effective-site-blocking.

14. A study conducted on three waves of site-blocking orders issued in Korea in 2014 and 2015 determined that they had resulted in an average decrease of 90 per cent in visits from users in Korea to the piracy websites subject to the orders.[20]

15. In Australia, the number of site-blocking orders has increased significantly since late 2018. A study on the impact of orders issued between 2018 and 2020 concluded that site blocking had contributed to a 5 per cent increase in traffic to legal streaming sites.[21] An earlier study of orders issued between December 2016 and February 2018 found that visits by users in Australia to blocked sites had dropped by 68.7 per cent. Moreover, visits to and usage of the 250 most popular piracy websites (including those not subject to blocking orders) in Australia had decreased by 42 per cent.[22]

16. Research in Europe has shown similar results. A study of three waves of site-blocking orders issued in the United Kingdom between 2012 and 2014 showed that the first blocking order of just one website in 2012 failed to bring about a decrease in visits to piracy websites or increase in usage by UK residents of legal sites and online services. That changed in 2013, when site-blocking orders were issued against 19 additional piracy websites, resulting in both a decrease in visits to such websites overall and an increase in the use of legal websites and services. The issue of site-blocking orders in 2014 against an additional 53 piracy websites had a significant impact. Overall, the number of visits to piracy websites dropped and usage of legal subscription services rose by 7-12 per cent. The number of new subscriptions to such legal services also increased.[23]

17. In the Nordic countries in Europe, Mediavision conducts an annual study on trends in the illegal use of audiovisual content in those countries. The latest study, released in 2023, shows an increase in illegal use across all Nordic countries between 2021 and 2023. That is due in part to the emergence of several new forms of online audiovisual piracy, such as “stream ripping”, illegal IPTV and more sophisticated piracy operations spread across multiple servers. While Finland currently has the lowest levels of piracy among the Nordic countries, Denmark, which previously held that position, continues to demonstrate the effectiveness of its anti-piracy efforts. Its dynamic blocking injunction tool, which allows for swift and adaptive blocking of piracy sites, has been instrumental in combating piracy despite regional increases in the last few years. It should be taken into account that Denmark has one of the highest Internet penetration rates[24] and fastest average fixed broadband Internet download speeds worldwide.[25]

18. Experience shows that site blocking leads to a reduction in the number of monthly visits to the illegal services in question by an average of 70 per cent in the four to five months following the issue of a site-blocking order against the ISPs. The following figure illustrates the decrease in the number of visits to blocked websites following six Danish court rulings issued in 2019.

---

20 MPA, “Study on Site Blocking Impact in South Korea”, 2016, https://www.mpa-apac.org/wp-content/uploads/2018/01/MPAA_Impact_of_Site_Blocking_in_South_Korea_2016.pdf.

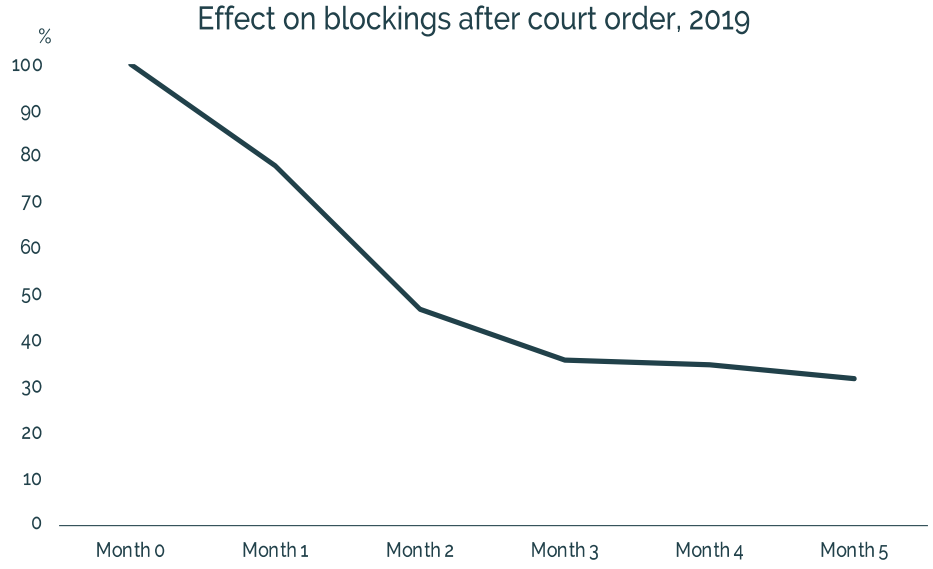
21 Cory, Nigel, “A Decade After SOPA/PIPA, It’s Time to Revisit Website Blocking”, Information Technology & Innovation Foundation, January 2022, https://itif.org/publications/2022/01/26/decade-after-sopa-pipa-time-to-revisit-website-blocking/.

22 Incopro, “Site Blocking Efficacy—Key Findings Australia”, July 2018, https://creativecontentaustralia.org.au/wp-content/uploads/2021/03/INCOPROAustralianSiteBlockingEfficacyReport-KeyFindingsJuly2018FINAL.pdf.

23 Danaher, Brett; Hersh, Jonathan; Smith, Michael D.; Telang, Rahul, “The Effect of Piracy Website Blocking on Consumer Behavior”, August 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612063.

24 Countries with the highest Internet penetration rate 2024 | Statista.

25 Global: fastest fixed Internet speed by country 2024 | Statista.



19. The Information Technology and Innovation Foundation has summed up the effectiveness of site blocking as follows: "Systems need to block access to a broad range of major piracy sites to be truly effective in shifting people to legal content providers."[26] When blocking orders issued by a country apply to a significant number of popular piracy websites (and their mirror and proxy sites[27]), then visits by users in that country to piracy sites decrease and use of legitimate content websites and online services increases. As the High Court of Delhi has noted, "there is a reason why website blocking is being used in a growing number of countries: It can be a reasonable and useful tool to reduce piracy and encourage the consumption of legal content."[28]

III. LEGAL BASIS FOR SITE-BLOCKING ORDERS

20. The legal basis for site blocking has been developed and refined over the years. This section identifies some of the relevant treaties, legislation and case law that provide the legal basis for site blocking around the world.

A. INTERNATIONAL TREATIES

21. As digital technologies developed and the Internet emerged in the late 20th century, international treaties were adopted to clarify copyright and to address the enforcement challenges posed. The WIPO Copyright Treaty[29] provides for the right of communication to the public. Under Article 8 of the Treaty, that right includes "the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them". Thus, a copyright owner has the exclusive right to authorize or deny making his or her work available online and, on the Internet,

---

[26] Corey, Nigel, "A Decade After SOPA/PIPA, It's Time to Revisit Website Blocking", Information Technology & Innovation Foundation, January 2022, https://itif.org/publications/2022/01/26/decade-after-sopa-pipa-time-to-revisit-website-blocking/.

[27] A mirror site is an identical or nearly identical copy of the original website hosted on a different server. A proxy site is a "work around" intermediary site or server that re-directs to a website that is the subject of a blocking order.

[28] *UTV Software Communication Ltd. and others v. 1337X.To and others*, High Court of Delhi, April 10, 2019, https://indiankanoon.org/doc/47479491/.

[29] Adopted in Geneva, on December 20, 1996, https://www.wipo.int/wipolex/en/text/295166#P97_14598.

which in turn serves as a legal basis for blocking site because of infringements of that right of communication to the public.

22. Under Article 14, the Contracting Parties must adopt measures to ensure effective remedies for copyright infringements, including to prevent future infringements. Article 14(2) states that "Contracting Parties shall ensure that enforcement procedures are available under their law so as to permit effective action against any act of infringement of rights covered by this Treaty, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements".

23. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement),[30] which came into effect in January 1995, also provides minimum standards for World Trade Organization (WTO) member States with regard to the protection of IPRs, including copyright. In particular, the TRIPS Agreement prescribes the obligation to implement measures at the national level that enable rights holders to enforce their rights. The standards are minimum standards, meaning that members may establish higher levels of enforcement. Furthermore, the TRIPS Agreement provisions are subject to the WTO dispute settlement mechanism.

24. Article 41 of the TRIPS Agreement[31] contains the following basic principles on the enforcement of IPRs: (i) the procedures must permit effective action against present and future infringements, including remedies that will deter further infringements; (ii) the procedures must be fair and equitable, and not unnecessarily complicated, costly, burdensome, or likely to cause unwarranted delays; (iii) courts and administrators must base their decisions on evidence available to all the parties and the decisions must be rendered in a timely manner, preferably in the form of a written, reasoned opinion; and (iv) member States must provide judicial appeal/review options for decisions made by administrative authorities.

25. The WIPO Copyright Treaty (WCT) and the TRIPS Agreement address the need for effective and expeditious actions and remedies to combat current and future infringements of copyright. Those principles provide a foundation for legal actions, such as site-blocking orders imposed on ISPs.

B.

26. The legal basis for blocking copyright infringing websites and online services in the European Union has been in place since 2002, when Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society (Information Society, or InfoSoc, Directive) came into force.[32] The InfoSoc Directive implements the WCT obligations and, together with Directive 2004/48/EC on the enforcement of IPRs (EU Enforcement Directive), sets out in detail the mechanisms and remedies that must be available in all EU member States.

27. The key provision of the InfoSoc Directive that serves as the legal basis for site blocking is Article 8(3). It provides that "Member States shall ensure that rights holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right". That mandate allows copyright holders to seek injunctions against Internet intermediaries that are used by copyright infringers to facilitate or promote their infringing activity *without* having to establish liability on the part of the intermediary itself. The mere provision of a service used by third parties for copyright infringements is sufficient. That "no fault injunction" approach has served not only as a basis for site-blocking orders against

30 https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm.
31 https://www.wto.org/english/docs_e/legal_e/trips_e.htm#part3.
32 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32001L0029.

ISPs across EU member States. It has also provided the basis for injunctions against hosting providers to terminate their services to infringing websites,[33] against search engines to de-list and remove piracy websites from their search results[34] and against domain name registrars to suspend the domain names of piracy websites.[35] In such cases, the intermediaries concerned were subject to the jurisdiction of the courts that issued the orders.

28. Under EU law, intermediaries such as ISPs and hosting providers may fall within the safe harbor rules set forth in Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market (E-commerce Directive).[36] Articles 12 to 15 of the Directive exempt such intermediaries from liability provided that they comply with certain criteria. Nevertheless, that liability exemption neither counters nor diminishes the possibility of obtaining injunctions against such intermediaries pursuant to the InfoSoc Directive. That is because the exemptions (such as for "mere conduits") only regulate the liability of the intermediaries, without prohibiting or limiting no-fault injunctions against intermediaries.[37] Because site-blocking injunctions are independent of liability, they are not affected by those liability exemptions.

29. Recital 59 of the InfoSoc Directive provides a clear rationale for site-blocking orders against ISPs. It explains the need for a "no fault injunction" approach that allows rights holders to obtain injunctions against Internet intermediaries without a requirement to establish any legal liability on the part of such intermediaries: "In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases, such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rights holders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This possibility should be available, even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States."

30. The EU directives provide member States with some discretion with regard to the procedures for issuing site-blocking orders. In most member States, the courts issue site-blocking orders after legal proceedings initiated by rights holders. In Greece, Italy and Portugal, however, the law provides for administrative site-blocking orders.[38] In those countries, rights owners may file a complaint with a government agency or regulatory authority that has the power to issue site-blocking orders. Such administrative procedures are usually faster and less expensive than seeking site-blocking orders from courts. For example, in Italy, AGCOM, the national communications regulatory authority, has a special "fast-track" procedure for websites involved in massive copyright infringements, whereby AGCOM must decide whether to issue the site-blocking order within 12 working days.[39] The administrative proceedings for site

---

[33] See *Twentieth Century Fox Film Corporation v. Voxility S.R.L.*, File No 36942/3/2013, Bucharest Tribunal – 3rd Civil Section, 22 September 2014 (translated from Romanian).

[34] See www.editionmultimedia.fr/wp-content/uploads/2013/12/Décision-Allostreaming-du-TGI-Paris-le-28-11-13.pdf.

[35] A reference to the Luxembourg case can be found in this article: Putlocker loses domain name following court order, https://torrentfreak.com/putlocker-loses-domain-name-following-court-order-170228/.

[36] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031.

[37] Judgment of 15 September 2016, *Tobias McFadden v. Sony Music Entertainment*, C-484/14, EU:C:2016:170, paras. 79 and 101, https://curia.europa.eu/juris/document/document.jsf?text=&docid=183363&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7284879.

[38] Corey, Nigel, "A Decade After SOPA/PIPA, It's Time to Revisit Website Blocking", Information Technology & Innovation Foundation, January 2022, https://itif.org/publications/2022/01/26/decade-after-sopa-pipa-time-to-revisit-website-blocking/.

[39] Kluwer Copyright Blog, "Italian public enforcement of online copyright infringement: new powers and procedures for AGCOM", December 2018, https://copyrightblog.kluweriplaw.com/2018/12/14/italian-public-enforcement-of-online-copyright-infringement-new-powers-and-procedures-for-agcom/.

blocking are often based on pre-established procedural and material criteria that provide reasonable certainty to the rights holder regarding the decision following a request for blocking. In accordance with Article 41 of the TRIPS Agreement, site-blocking administrative decisions are normally subject to judicial appeal or review. Annex 2 provides a deeper dive into the administrative site-blocking procedures in Italy, Portugal and the Republic of Korea.

31. In key decisions, the Court of Justice of the European Union (CJEU) has transformed the more general legal principles from EU directives and international treaties into practical rules and guidelines that are applicable to all EU member States when addressing site-blocking orders. In the landmark *UPC Telekabel v. Constantin* decision of 2014,[40] the CJEU set forth the following key principles:

(a) An ISP does **not** need to have any business relationship with a piracy website or operator of such a website to be subject to a site-blocking order. As stated by the CJEU, "neither the wording of Article 8(3) nor any other provision of Directive 2001/29 indicates that a specific relationship between the person infringing copyright, or a related right and the intermediary is required".

(b) Rights holders do **not** need to establish that customers of the ISP actually accessed the relevant copyright-infringing website to secure and justify a site-blocking order. According to the CJEU, "holders of copyright or of a related right may act without having to prove that the customers of an internet service provider actually access the protected subject matter made available to the public without their agreement."

(c) It is not necessary for all, or even a majority of, the rights holders whose rights are infringed on the website to file for a blocking order. Usually, just one or a small group of rights holders applies for a blocking order against a website that contains much more infringing content than just those works for which the plaintiff(s) own rights. As long as the primary purpose or primary effect of the site is illegal, then a blocking order will be issued.[41]

(d) Site-blocking orders issued against websites engaged in blatant copyright infringement are justified and properly balanced against the fundamental freedom to conduct a business and the fundamental freedom of information. As noted by the CJEU, a site-blocking injunction "makes it necessary to strike a balance, primarily, between (i) copyright and related rights, which are intellectual property and are therefore protected under Article 17(2) of the Charter [of Fundamental Rights of the European Union], (ii) the freedom to conduct a business, which economic agents such as Internet service providers enjoy under Article 16 of the Charter, and (iii) the freedom of information of Internet users, whose protection is ensured by Article 11 of the Charter". The CJEU concluded that "the fundamental rights recognized by EU law must be interpreted as not precluding a court injunction prohibiting an internet service provider from allowing its customers access to a website placing protected subject matter online without the agreement of the rightholders".

(e) Site-blocking orders do **not** have to reduce overall piracy or be incapable of circumvention. The CJEU specifically acknowledged "that a means of putting a complete end to the infringements of the intellectual property right does not exist or is not in practice achievable, as a result of which some measures taken might be capable of being circumvented in one way or another". It thus held that site-blocking orders are justified when they make it difficult for users of the ISP subject to the

---

40 *UPC v. Constantin*, Case C-314/12, https://curia.europa.eu/juris/document/document.jsf?docid=149924&doclang=EN.

41 Norwegian Premier League-case (18-039103TVI-OTIR/02) and Danish La Liga-case (BS-5975/2019-FRB).

blocking order from accessing the relevant website(s), or "seriously discourage" them from doing so.

32. In 2017, the CJEU reissued another important judgment on site blocking[42] in the case of The Pirate Bay website. That website does not host copyright-infringing content. Rather, it provides an index of data and a search engine relating to copyrighted works for which users of the website have uploaded BitTorrent peer-to-peer file-sharing links that permit other users of the BitTorrent file-sharing protocol to locate those works and download them. The CJEU held that site-blocking orders may be issued against websites such as The Pirate Bay based on the following principles:

(a) Websites do **not** have to host infringing content in order to be engaged in unauthorized acts of communication to the public of copyright-infringing content. The CJEU held that "the operators of the online sharing platform The Pirate Bay, by making that platform available and managing it, provide their users with access to the works concerned … and can therefore be regarded as playing an essential role in making the works in question available." That is the case even though the links to the works are uploaded to the platform "not by the platform operators, but by its users".

(b) Websites do **not** have to be wholly devoted to copyright infringement in order to be subject to site-blocking orders. The CJEU found it sufficient that the torrent files offered on The Pirate Bay "relate mainly to copyright-protected works, without the rightholders having given their consent to the operators or users of that platform to carry out the sharing acts in question."

33. In 2021, the CJEU clarified that exploitation of a video-sharing platform, such as YouTube, by users to infringe copyright does not necessarily mean that the platform's operator has engaged in an unauthorized act of communication to the public.[43] Rather, there needs to be some level of knowledge and complicity on the part of the website/platform operator. Nevertheless, even when no such knowledge or complicity is involved, targeted, "no-fault" injunctive relief other than site blocking can still be ordered. Such relief could come in the form of an order requiring that the website remove the infringing content if the website operator falls within the jurisdiction of the court concerned.[44]

---

[42] Judgment of 14 June 2017, *Stichting Brein v. Ziggo*, C-610/15, EU:C 2017:456 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0610).

[43] Judgment of 22 June 2021, *Peterson v. YouTube* and *Elsevier v. Cyando*, joint cases C-682/18 and C-683/18, EU:C:2021:503 (https://curia.europa.eu/juris/document/document.jsf?docid=243241&doclang=en). The CJEU held that "the operator of a video-sharing platform or a file-hosting and sharing platform, 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."

[44] It is unlikely that a site-blocking order would be issued in such a case, unless the vast majority of the content made available on the platform by the users infringed copyright.

34. Lastly, it seems that site-blocking orders may also be imposed on websites engaged solely in the sale of certain equipment or hardware. In the Filmspeler case, although site blocking was not at issue, the CJEU held that the sale of a media player can constitute an illegal act of communication to the public.[45]

35. In the Filmspeler case, the defendant had pre-installed on the media player boxes he sold software developed and made available by third parties giving users easy access to stream copyrighted works made available online without the rights owners' authorization. Although that open-source software was available online and was not altered by the defendant, and the software connected to publicly available websites hosting pirated content, the CJEU still found that the sale of the media players by the defendant infringed copyright. The CJEU held that, by installing the software on the media players and then advertising the latter as giving customers free access to popular content that would normally require a paid subscription, the sale of the media players alone constituted an illegal act of communication to the public in violation of the rights of the copyright holders. In reaching that decision, the CJEU rejected the argument that the sale of the media players constituted the provision of "mere physical facilities". Rather, the CJEU held that, given the full knowledge (and indeed advertising) of the media players' ability to facilitate infringing activity and the sale of the device for profit, the communication to the public right "must be interpreted as covering the sale of a multimedia player, such as that at issue in the main proceedings, on which there are pre-installed add-ons, available on the Internet, containing hyperlinks to websites — that are freely accessible to the public — on which copyright-protected works have been made available without the consent of the rights holders".[46] In that light, it seems that courts in EU member States could issue site-blocking orders against foreign websites devoted solely or primarily to the sale of such infringing devices.

36. Those and other decisions by the CJEU have enabled national courts in EU member States to impose site-blocking orders on ISPs (including broadband operators both mobile and stationary) with respect to a broad array of websites and online services purposely engaged in activities that facilitate copyright infringement. They include websites that host content, websites that merely supply links to content, websites that index and organize peer-to-peer file sharing links of content, apps and services that facilitate the unauthorized streaming of content, and websites that permit the unauthorized streaming of broadcasts of live events, such as sporting events.[47] Across the EU, site-blocking orders are becoming a more prevalent tool for enforcing copyright.

C. ASIA-PACIFIC

37. Site blocking has been adopted so far by nine countries in the Asia-Pacific region. In this section we focus on Australia, the Republic of Korea, India and Indonesia. Australia and India were chosen because of the comprehensive judicial opinions issued by courts in both countries. The Republic of Korea provides an example of where an administrative procedure has been adopted. Lastly, Indonesia was selected because the multiple waves of site-blocking orders there have led to the blocking of thousands of piracy websites.

38. In Australia, the Copyright Act specifically provides for "no fault" injunctive relief in the form of site blocking. Under Section 115A of the Copyright Act, as amended in December 2018, copyright owners may apply to the Federal Court for an injunction against ISPs requiring

---

45 Judgment of April 26, 2017, *Stichting Brein v. Wullems*, C-527/15, EU:C:2017:300 (https://curia.europa.eu/juris/document/document.jsf?text=&docid=190142&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=2784868).

46 Ibid.

47 For examples of such decisions, see EUIPO "Study on Dynamic Blocking Injunctions in the European Union", March 2021, https://www.euipo.europa.eu/en/publications/dynamic-blocking-injunctions-in-the-eu.

them to take steps deemed reasonable by the Court to disable access to an online location outside Australia that

> (a) infringes, or facilitates infringement, of copyright; and
>
> (b) has the primary purpose or the primary effect of infringing, or facilitating infringement, of copyright (whether or not in Australia).[48]

39. As stated by the Federal Court in the Roadshow Films case, Section 115A "provides for a 'no fault' remedy against a [ISP]. In particular, the entitlement of an applicant for relief under S[ection] 115A does not depend upon it establishing that the [ISP] against which it seeks such relief has committed an infringement of copyright either by its own acts or by authorizing the acts of another person."[49] Courts in Australia have held that site-blocking orders are not limited to piracy websites hosting infringing content. Rather, they can also apply to a website or online location, the primary purpose of which is to "facilitate the infringement of copyright merely by making it easier for users to ascertain the existence or whereabouts of other online locations that themselves infringe or facilitate the infringement of copyright".[50] Thus, site-blocking orders have been issued for BitTorrent indexing sites such as The Pirate Bay and Torrentz.[51] They have also been issued against websites offering apps and services that facilitate infringement. One example is a case where the court issued a blocking order against websites that "rip" music from music videos that were uploaded by the rights owners to YouTube solely for streaming ("stream ripping"). The websites allowed the users to "rip" the soundtracks from the YouTube streams and then download and copy them without the authorization of the copyright owners.[52]

40. In the Republic of Korea, the Copyright Act provides a legal basis for site-blocking. Under the Act, copyright holders can enforce their rights, including by means of injunctive relief for those whose works are being infringed.[53] Moreover, under the Act on Promotion of Information and Communications Network Utilization and Information Protection of 2012, the authorities may block access to online locations that infringe or facilitate the infringement of copyright.[54] One prominent method is Domain Name System (DNS) blocking, whereby ISPs are required to block access to specific domain names of piracy sites, including those located abroad.

41. In the case of *Korea Copyright Protection Agency (KCOPA) v. Naver Corp.*, the Supreme Court held that Internet platforms share responsibility for enforcing copyright.[55] The focus of the case was on the defendant's role in hosting and aggregating copyrighted content without proper authorization, but the Court also established the authority to issue site-blocking orders against ISPs facilitating infringement. It held that the Copyright Act enables rights holders to seek injunctive relief, including site blocking, to prevent further unauthorized distribution of their works. The Court used a qualitative approach to determine whether a website should be blocked, focusing on its primary purpose rather than relying on a quantitative analysis. If a

---

48 https://www5.austlii.edu.au/au/legis/cth/consol_act/ca1968133/s115a.html.

49 *Roadshow Films Pty Ltd v. Telstra Corporation Ltd* [2016], FCA 1503, https://wipolex-resources-eu-central-1-358922420655.s3.amazonaws.com/edocs/lexdocs/judgments/en/au/au050-jen.pdf.

50 Ibid., para. 47.

51 Ibid., paras. 98 and 108.

52 *Apra v. Telstra*, as analyzed in Ottaway, Harrison, "Internet (almost) killed the video star: Federal Court grants orders to block 'ripping' of music videos", June 2019, The Brand Protection Blog, https://www.thebrandprotectionblog.com/2019/06/internet-almost-killed-the-video-star-federal-court-grants-orders-to-block-ripping-of-music-videos/.

53 Copyright Act of the Republic of Korea (Arts. 125 and 136).

54 https://wilmap.stanford.edu/entries/act-promotion-information-and-communications-network-utilization-and-information-protection.

55 *Korea Copyright Protection Agency v. Naver Corp.*, Supreme Court of Korea, Case No. 2016Da40100, 2016 (Republic of Korea).

website primarily facilitates copyright infringement, it can be blocked, regardless of any legal content it may host from the Republic of Korea.

42. The Korea Communications Commission (KCC) plays a crucial role in facilitating compliance with blocking orders by notifying ISPs and coordinating with regulatory bodies for enforcement.[56] As infringing websites often attempt to evade blocking by changing domain names or creating mirror sites, courts have adopted dynamic site-blocking orders that allow copyright holders to submit affidavits detailing new domains associated with infringing activities, without the need for new court orders each time.

43. With the rapid increase in the number of foreign infringement websites, such as *Bamtoki*, which distributed Korean webtoons without authorization and outside the jurisdiction of the Republic of Korea in order to circumvent local laws, the need for more effective enforcement measures became apparent.[57] The Korea Copyright Protection Agency (KCOPA), working with the Ministry of Culture, Sports and Tourism, KCC and the Korea Communications Standards Commission KCSC), led several rounds of site blocking actions. The *Bamtoki* case is one of the most notable examples demonstrating the impact of site blocking measures, where traffic to the piracy site dramatically decreased, with reports showing a 97 per cent drop in the number of visitors between April and June 2018. Despite that success, the phenomenon of "balloon effects" soon became apparent, as users migrated to alternative piracy sites, forcing the Government to expand the list of blocked sites and adapt to the rapid evolution of new piracy platforms. Those efforts led to further rounds of site blocking, with some websites increasing their traffic as users sought out other illicit alternatives. Despite the challenges posed by those dynamic piracy tactics, site blocking remains a central part of the country's strategy for combating online copyright piracy.

44. In India, site-blocking orders for copyright infringement have been embraced under the Copyright Act and Section 79(3)(b) of the Information Technology Act.[58] In one key case, *UTV Software Communication Ltd. and others v. 1337X.To and others*, the High Court of Delhi concluded that it had the authority to issue site-blocking orders against ISPs on the basis of the Copyright Act alone.[59] The Court stated that "Section 55 of the Copyright Act provides civil remedies to the rights holders, which includes entitlement to an injunction order on approaching the Court. Consequently, the Court has ample inherent powers to mold the relief to ensure that the plaintiffs' rights as copyright owners are adequately protected."[60] That is significant, because it demonstrates that judicial authorities in some countries have determined that the standard provisions in copyright law concerning injunctive relief are adequate to support the granting of site-blocking orders without the need for legislation on "no fault" injunctive relief against Internet intermediaries or site blocking specifically.

45. The Court established other legal principles and guidelines with regard to site blocking that have led to its effective implementation in India. They include:

(a) The test for determining whether a website should be subject to site blocking "is a qualitative approach and not a quantitative one". If the primary purpose and effect of the website is to facilitate infringement, then the fact that the website might host or

---

[56] KCC Report on Copyright Enforcement, 2022, https://www.kcc.go.kr/user.do?mode=view&boardId=1053&page=E02020000&dc=E02020000&boardSeq=57095/.

[57] Korea Copyright Protection Agency Report, 2018, https://www.kcopa.or.kr/download.do?uuid=95535471-b706-4832-9809-f2468230a1db.pdf/.

[58] "Finding 404: A report on website blocking in India 2022", SFLC, in https://images.assettype.com/barandbench/2023-01/5b3b5f47-930a-4c78-b425-1109b7f12e08/Finding_404___A_Report_on_Website_Blocking_in_India.pdf.

[59] *UTV Software Communication Ltd. and others v. 1337X.To and others*, High Court of Delhi, April 10, 2019, https://indiankanoon.org/doc/47479491/.

[60] Ibid., para 49.

index some legal content is not relevant. It is the responsibility of the copyright owners, by providing sample evidence, "to prove to the satisfaction of the Court that each website they want to block is primarily facilitating widespread copyright infringement". Factors such as the lack of legitimate contact details for the website, that the website "hide[s] behind [a] veil of secrecy" and that the website provides instructions as to how to avoid detection for using or accessing it, can and should all be taken into account when applying the qualitative test.

(b) The website does not need to host the infringing content. If, for example, it indexes torrent files or provides links in order to facilitate copyright infringement as its primary purpose, then that is adequate to justify a site-blocking order.

(c) To be effective and cost efficient, site blocking should be applied to entire websites, not to individual URLs.

(d) Government agencies should facilitate compliance with site-blocking orders. The Court ruled that it had the authority to instruct the Department of Telecommunications and the Ministry of Electronics and Information Technology to notify ISPs in India of site-blocking orders and help to implement them.

(e) Dynamic site-blocking orders are appropriate. The Court noted that piracy websites subject to blocking orders will often seek to avoid them by operating mirror sites or redirect websites operating under new domain names that re-direct to the original piracy website, and by employing other similar tactics. The Court therefore ruled that its site-blocking order should be a dynamic one that takes account of those tactics. Thus, copyright plaintiffs do not need to seek new court orders to address the additional websites. Instead, they may submit an affidavit to an administrative authority appointed by the Court that identifies the new domain names and/or IP addresses and attests that "they merely provide new means of accessing the same primary infringing websites that have been injuncted". The additional websites are then added to the blocking order.

46. In Indonesia, the law provides for administrative site blocking, which is carried out by the Ministry of Communication and Informatics (KOMINFO).[61] Instead of a judicial process, copyright owners submit applications to the Directorate General of Intellectual Property (DGIP), identifying copyright piracy websites and providing supporting evidence/statements. If DGIP approves the application, it forwards the blocking request to KOMINFO, which in turn orders the ISPs to block the sites.[62] According to a report from the Information Technology and Innovation Foundation, "beginning in 2019, the Indonesian regulator KOMINFO began a massive wave of website blocking in conjunction with the Video Coalition of Indonesia. Over the course of 2019-2020, over 2,300 piracy sites were blocked, averaging 60 sites blocked every 10 days. Due to these efforts, Indonesia has the lowest levels of illicit streaming device usage in the Asia-Pacific, second only to Singapore. In the year following the start of this 'rolling' site blocking, visits to piracy sites fell by 55 per cent."[63] By April 2022, more than 3,500 piracy websites had been blocked in Indonesia. At that time, the Asia Video Industry Association reported that "76 per cent of Indonesian consumers say they are accessing more legal content and pirating less, and 26 per cent say they have subscribed to legitimate sources as a result of illegal streaming sites

---

61 UK Intellectual Property Office, "Guidance: IP enforcement in Indonesia", October 2023, https://www.gov.uk/guidance/ip-enforcement-in-indonesia.

62 Redfearn, Nick, "Content and Site Blocking in SE Asia", ROUSE, November 2023, https://rouse.com/insights/news/2024/content-and-site-blocking-in-se-asia#:~:text=Indonesia,to%20the%20ISP%20or%20website.

63 Corey, Nigel, "A Decade After SOPA/PIPA, It's Time to Revisit Website Blocking", Information Technology & Innovation Foundation, January 2022, https://itif.org/publications/2022/01/26/decade-after-sopa-pipa-time-to-revisit-website-blocking/.

being blocked. Blocking as an educational tool may also be evident in 95 per cent of Indonesian consumers agreeing that online piracy does have negative consequences – the highest in the region."[64]

D. LATIN AMERICA

47. Site blocking has been adopted by at least nine countries in Latin America. Argentina, Brazil and Uruguay will be the focus of this section. The regime in Argentina has evolved and expanded over time. Site blocking in Brazil is based on both civil and criminal law and involves a mixture of court-ordered site blocking and site blocking performed by administrative agencies. Uruguay is one of the few countries in Latin America with specific legislation that provides for site blocking — including dynamic blocking orders and the blocking of streaming of live events, such as sports broadcasts — via an efficient administrative process.

48. The first website-blocking order issued in Latin America was in Argentina in 2011. The case concerned a piracy website called Cuevana, a very popular file-sharing site that offered movies and television programs with Spanish subtitles. Rights holders brought a civil lawsuit against Cuevana[65] and the Federal Court of First Instance issued a blocking order as a precautionary measure on the basis of Article 79 of the copyright law of Argentina, Law No. 11.723.[66] Article 79 covers seizures aimed at protecting rights. Argentina was also the first country in Latin America to block The Pirate Bay.[67] The 67th District Federal Court issued the blocking order based on Articles 71 and 72(a) of Law No. 11.723, which address general penalties for infringement. There is no specific language in Law No. 11.723 that provides for site blocking or for "no-fault" injunctive relief against ISPs and other Internet intermediaries for copyright infringement committed by third parties that use their services. Pursuant to the order of the District Federal Court, the National Communications Commission ordered all ISPs in Argentina to block 256 IP addresses of The Pirate Bay and 12 domain names, including thepiratebay.org, thepiratebay.com, thepiratebay.se and thepiratebay.de.[68] In Argentina, site-blocking orders are issued both by civil federal courts and criminal courts. These site-blocking court orders are then communicated to all ISPs and overseen by the National Communications Agency (Ente Nacional de Comunicaciones – ENACOM).

49. In December 2022, the National Court of First Instance in Federal Civil and Commercial Matters ordered the blocking of 30 domain names of piracy websites, many of which were illegal television streaming services and portals dedicated to the unauthorized transmission of linear pay-television channels and sporting events.[69] The Court in this case issued a dynamic blocking order, permitting new mirror and re-direct domains and websites that are subject to the order to be quickly added and efficiently blocked without the need to bring a new lawsuit. Notably, beyond mirror and re-direct websites, the order also permits the plaintiff rights holders to submit, on a monthly basis, a list of the 30 most popular piracy websites and services involved in the transmission of illegal IPTV, live events and other audiovisual programming that infringes the rights of the plaintiffs. These new websites are then added to the site-blocking order without the need for a new court proceeding. As noted in an article about the case, it sets "a significant

---

64 See https://avia.org/indonesia-continues-to-lead-the-way-in-site-blocking/.

65 Imagen Satelital SA, C/ Quien Resulte Titular Sitio Web Cuevana S/ Medidas Precautorias

66 https://www.cij.gov.ar/nota-8304-Ordenaron-bloquear-el-acceso-a-tres-series-en-el-sitio-web-Cuevana.html.

67 See: https://torrentfreak.com/the-pirate-bay-now-blocked-in-argentina-140701/.

68 *Ibid*.

69 DIRECTV ARGENTINA SA Y OTROS c/ QUIEN RESULTERESPONSABLE DE LOS NOMBRES DE DOMINIO s/MEDIDAAUTOSATISFACTIVA, available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://torrentfreak.com/images/MedidaBloqueoSenales.pdf. See also: https://torrentfreak.com/copyright-holders-score-dynamic-pirate-site-blocking-order-in-argentina-230207/ and https://www.dataclave.com.ar/poder/un-fallo-historico-en-argentina-bloquea-sitios-piratas-que-transmitian-futbol-ilegalmente_a63ff68069bd5588254386a15.

precedent that will allow for regular updates to the list of illegal sites to be blocked in Argentina."[70]

50. In September 2024, Argentina developed its site-blocking program further, beyond dynamic blocking, with a case involving illicit television boxes that were used to illegally access signals from legitimate cable operators, as well as the piracy IPTV service Magis TV.[71] The Magis TV service has been described as follows: "Magis TV is believed to operate out of China. Its focus is on the Latin American market where millions consume content mostly via the [Magis TV] platform's ubiquitous, subscription-based Android app."[72] The case began as a criminal investigation and prosecution of individuals selling illegal preloaded television boxes, including some with the Magis TV app already installed. The court then ordered the blocking of 69 domain names associated with Magis TV, including websites engaged in reselling subscriptions to Magis TV services, websites engaged in selling the Magis TV app, and other MagisTV-related websites. Beyond this site blocking, however, the court also ordered Google, the primary developer and system operator of the Android system, to disable or uninstall existing Magis TV apps on all Android devices registered in Argentina. The court ordered Google to "adopt the necessary technical means to immediately uninstall from Android systems that report IP addresses in the territory of the Argentine Republic (which can be verified by the IP addresses assigned to this country), the application named Magis TV."[73] This is a groundbreaking development in the legal regime for site blocking because it is the first time that a court has ordered, in conjunction with a site-blocking order applicable to ISPs, the removal of apps already installed on various devices by the infrastructure provider — in this case Google — responsible for the operating system on Android devices.[74] Indeed, the prosecutor involved in the criminal action stated that "this has never been done before. What was achieved is an unprecedented court order…which is to uninstall, through the Android operating system update, the application on all devices that have an IP address in Argentina."[75] Only time will tell whether this expanded approach, enabling operating system providers to be ordered to disable or uninstall piracy apps, will be adopted by other countries.

---

70 See: https://marcasur.com/en/noticia.php?ID=4062&f=-2023.

71 Case: PP-14-00-005453/24, "Viñales Roberto Horacio s/ Infracción a la Ley 11.723".

72 https://torrentfreak.com/magis-tv-iptv-crackdown-blocks-70-domains-hundreds-already-wiped-out-240918/.

73 https://torrentfreak.com/court-orders-google-to-uninstall-pirate-iptv-app-sideloaded-on-android-devices-240923/.

74 *Ibid*.

75 *Ibid*.

51. In addition, the court in the Magis TV case also ordered the seizure of the domain name of the piracy website that was registered with the Argentine country code: Top-Level Domain (TLD) .ar. The court ordered the registry of .ar to transfer the domain todotechno.com.ar to the Prosecutor's Office. As a result, when users typed the domain name into their browsers, they were taken to a landing page informing them that the domain had been seized owing to illegal activity. Here is an image of the landing page:

52. In Brazil, site-blocking orders are currently based on the general provisions of the country's copyright law and are often issued in conjunction with criminal investigations involving copyright infringement.[76] Since 2019, courts in Brazil have issued site-blocking orders in waves, referred to as Operation 404 (404 is a reference to a typical online error message that reads "404 Not Found" when a website cannot be located by the domain name, URL or IP address typed into a browser). As of September 2024, there have been seven phases of Operation 404, each of which has resulted in the blocking of hundreds of piracy websites.[77]

53. In addition to piracy websites, blocking orders in Brazil have been issued with respect to illegal IPTV streaming services, stream-ripping platforms and piracy apps.[78] In Phase 7 of Operation 404, search engines were ordered to de-index piracy websites and pages related to copyright piracy were ordered to be removed from social media networks.[79] Under Article 184 of the Brazilian Penal Code, the unauthorized distribution of copyrighted works may result in prison sentences of 2 to 4 years.[80] Furthermore, these criminal copyright investigations, which regularly lead to court-ordered site blocking, often involve coordination between multiple law enforcement agencies in Brazil and collaborations with law enforcement agencies in other

[76] Note that while a law was passed in Brazil (Law No. 14.815/24) to establish a specific administrative procedure for site blocking based on copyright infringement that would empower the Agencia Nacional do Cinema (ANCINE) to issue site-blocking orders, the regulation to define the administrative process has not yet been implemented and is still pending.
[77] See: https://piracymonitor.org/brazil-announces-phase-7-of-operation-404-first-wins-under-operation-redirect/.
[78] See: https://torrentfreak.com/operation-404-7-targets-675-pirate-sites-brazil-now-blocks-6700-domains-240920/.
[79] See: https://piracymonitor.org/brazil-announces-phase-7-of-operation-404-first-wins-under-operation-redirect/.
[80] See: https://www.clarkemodet.com/en/articles/operation-404-7-a-successful-international-crackdown-on-digital-piracy/.

countries, as well as associations of copyright and IPR holders and stakeholder groups for IP protection.[81]

54. Site-blocking orders in Brazil are not only granted by courts. The National Telecommunications Agency (Agência Nacional de Telecomunicações – ANATEL), the telecommunications regulatory agency of Brazil, issues administrative site-blocking orders with respect to illegal IPTV services and piracy apps loaded into illicit and non-certified set-top television boxes and the illegal television boxes themselves. The authority of ANATEL with respect to site blocking is limited to online websites, servers and apps associated with illegal piracy set-top television boxes. The blocking injunctions are based on the lack of approval of such television boxes by ANATEL and the risks to end users (e.g., lack of parental controls and content classifications, lack of security for personal data). ANATEL announced that, as of October 2023, over 3,000 servers enabling millions of piracy television boxes had been blocked in Brazil.[82] As of October 2024, ANATEL had blocked more than 13,500 domain names and IP addresses and is coordinating live "real-time" blocking actions to be executed during live sports events.

55. In Uruguay, the first site-blocking order was issued in 2018 by the Criminal Court of First Instance Specialized in Organized Crime ("the Criminal Court") as a precautionary measure.[83] The case concerned the website ROJADIRECTA, on which live sports events were illegally streamed and made available to its users via links to retransmissions of matches from all over the world without the authorization of the rights holders. It was a very popular website and Fox International Channels, the holder of the exclusive broadcast and transmission rights of several Latin American football/soccer events, filed a criminal complaint with the Criminal Court in 2017. Subsequently, the Public Prosecutor determined that ROJADIRECTA had violated the criminal provisions of Law No. 9.739, the copyright law of Uruguay, specifically its Article 46, and urged the Criminal Court "to decree the blocking of the access of the websites denominated ROJADIRECTA." The Criminal Court thus ordered the site to be blocked as a precautionary measure "to prevent the [copyright] violation from being committed or repeated," as provided by Article 48 of Law No 9.739, for all ISPs operating in Uruguay.[84]

56. While this first site-blocking order in Uruguay was based on the general provisions of the country's copyright law, Uruguay subsequently created a specific system of administrative site-blocking for illegal streams or rebroadcasts of subscriber television services. Article 712 of Law No. 19.924, promulgated in 2020, specifically empowers the government telecommunications agency, the Regulatory Unit for Communications Services (Unidad Reguladora de Servicios de Comunicaciones – URSEC), to issue such site-blocking orders.[85] Decree No. 345/22, issued in 2022 by the Ministry of Industry, Energy and Mining, provides that once URSEC has evaluated a complaint about illegal TV streams or other audiovisual piracy websites and services and is satisfied of their illegal nature, it will instruct ISPs to block the relevant websites and services, with ISPs required to implement such blocking orders within four days.[86] In addition, the Decree allows not only copyright holders to submit complaints to URSEC, but also licensed television operators. Furthermore, the Decree sets forth that site blocking may be required on the basis of IP addresses, domain names or URLs.[87] As a result, blocking orders

---

81 *Ibid*.

82 See: https://torrentfreak.com/brazil-regulator-claims-80-of-pirate-tv-boxes-were-blocked-last-week-231030/.

83 Cervieri, Virigina, "ISPs Forced to Block Illegal Streaming Website in Uruguay", Kluwer Trademark Blog, 16 May 2019, https://trademarkblog.kluweriplaw.com/2019/05/16/isps-forced-to-block-illegal-streaming-website-in-uruguay/.

84 Cervieri Monsuarez, "Precautionary Measure Locked Access to Web Sites That Reproduced TV Signals Without Paying", Case Law/Reporte, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cervierimonsuarez.com/repo/arch/2018reporterojadirectaeng.pdf.

85 https://www.impo.com.uy/bases/leyes/19924-2020/712.

86 See: https://torrentfreak.com/new-pirate-site-blocking-law-allows-intermediaries-to-file-complaints-221204/.

87 *Ibid*.

are also issued with respect to content-hosting websites and URLs that are involved with the logins and other functions of piracy apps related to illegal television and video services.

57. In October 2022, Uruguay passed a new law (Article 233, Law No. 20075) that allows URSEC to issue live site-blocking orders to disable real-time access to illegal live broadcasts of sporting events online.[88] A Presidential Decree related to this Law noted that "it is becoming increasingly simple to reproduce, distribute, publish, transform, communicate or make sporting events available to the public by a natural person or legal entity that is not authorized to offer them, violating rights protected by our legal system" and that "there are currently different alternatives that are constantly evolving to access and share content without the proper authorizations, making it essential to adopt actions that tend to protect the protected legal asset."[89]

58. The administrative site-blocking regime of Uruguay is based on these specific laws and decrees, and has been praised for its efficiency and transparency.[90]

59. For a summary of countries that have adopted site-blocking measures, as of January 2022, and a brief description of how their systems work, please see Annex 3.

E. FUNDAMENTAL CONCLUSIONS CONCERNING LEGAL BASES AND LEGAL PARAMETERS FOR SITE BLOCKING

60. Some fundamental conclusions that emerge from the review of treaties, statutory and legislative provisions, and case law are:

(a) Site-blocking orders are generally considered a civil remedy with respect to online copyright piracy, but are often issued in conjunction with criminal copyright cases as well.

(b) Site-blocking orders may be issued on the basis of statutory or legislative provisions that provide for "no fault" injunctive relief against Internet intermediaries for copyright infringement or on specific laws that authorize site-blocking orders to be imposed on ISPs. However, such statutory provisions are not a prerequisite for site blocking. Courts may also issue site-blocking orders on the basis of more general copyright laws that provide for injunctive relief. In addition, site-blocking orders have also been issued by courts on the basis of criminal laws relating to copyright infringement or the sale of illegal devices, such as illicit IPTV boxes or apps.

(c) Laws that provide liability protections or "safe harbors" for Internet intermediaries neither preclude nor limit the granting of site-blocking orders against ISPs.

(d) Websites and online services that are primarily devoted to facilitating or promoting copyright infringement are suitable for site blocking on the basis of their primary purpose or primary effect. They do not need solely to engage in or facilitate infringing activity. They do not need to host the infringing content and can instead be indexing sites, linking sites or the like. They can also include online apps, services or websites devoted to the sale of products that promote and facilitate copyright infringement. Moreover, the primary purpose can also be derived from, inter alia, the promotional statements of the websites or services, efforts to avoid identification, a

88 https://www.gub.uy/unidad-reguladora-servicios-comunicaciones/institucional/normativa/ley-n-20075-art-233-fecha-20102022-inhabilitacion-tiempo-real-del-acceso.
89 https://www.impo.com.uy/bases/decretos/324-2023/1.
90 See: https://torrentfreak.com/pirate-site-blocking-cant-prevent-pay-tv-subscriber-decline-in-uruguay-240806/.

lack of effective response to requests to remove infringing content or links to such content, and past legal actions brought against the websites or services in question.

(e) Site blocking can be accomplished through court orders or administrative procedures. More often, site-blocking orders are issued by courts.

(f) Rights holders have often found administrative procedures to be faster, less burdensome and less costly than civil litigations brought before courts and aimed at obtaining site-blocking orders.

(g) Rights holders seeking a site-blocking order need to establish that they hold the rights to the content that is subject to infringement by the website or service. There is no need, however, for all or even a substantial portion of the relevant rights holders of all the content being infringed by the website or service to be part of the action. Rather, those seeking the site-blocking order need to establish that the primary purpose or primary effect of the site or service is to facilitate copyright infringement.

(h) The costs of the technical implementation of site-blocking orders are usually borne by the ISPs. Site-blocking orders may prescribe the blocking method to be used or leave the method to employ to achieve the blocking to the discretion of the ISPs. A reasonable balance is generally sought between effectiveness and implementation cost.

(i) Dynamic orders that readily and quickly permit the addition of new domain names or IP addresses of websites or services that have already been subject to a blocking order are possible with respect to both judicial site-blocking orders and those imposed by administrative authorities. These dynamic orders allow rights holders to submit the new domain names or IP addresses under an accelerated process that permits the new domain names or IP addresses to be blocked quickly, in addition to the original domain names or IP addresses identified in the original blocking order. Courts and administrative agencies around the world have recognized that dynamic orders make site blocking more effective.[91] As noted in a recent study, piracy operators' efforts to evade and work around site-blocking orders "can be thwarted through dynamic site blocks that are able to evolve to capture any newly created domains and websites."[92]

(j) In recent years, some countries have been expanding the legal reach of their site-blocking regimes to include orders to Internet intermediaries beyond only access provider ISPs. The above-mentioned Magis TV case provides such an example with respect to Argentina. As described in Annex 2, AGCOM, the administrative agency in Italy responsible for issuing site-blocking orders, now has the legal authority to issue orders to other Internet intermediaries, such as: (i) VPN providers and alternative DNS resolvers to prevent users of such services from accessing blocked websites; (ii) reverse proxy service providers to suspend their services to blocked websites; and (iii) search engines to de-list blocked websites from search results (see Annex 2 for more details). This expanded approach, aimed at ensuring that other Internet intermediaries (beyond ISPs) do not allow their services to be used to find and access websites subject to blocking, increases the effectiveness of such

[91] See for example, EUIPO, "Study on Dynamic Blocking Injunctions in the European Union", March 2021, https://www.euipo.europa.eu/en/publications/dynamic-blocking-injunctions-in-the-eu.

[92] Mossoff, Adam, "Congress Should Protect the Rights of American Creators with Site-Blocking Legislation", The Heritage Foundation, February 2024, https://www.heritage.org/crime-and-justice/report/congress-should-protect-the-rights-american-creators-site-blocking.

site-blocking orders. This is particularly the case where — such as in Italy — orders against multiple intermediaries, along with ISPs, can be issued in a consolidated manner on the basis of a single complaint submitted by the rights holder.

61. Procedures for site-blocking orders depend on the national law of the country in question. However, the following are procedural characteristics that are often embraced in the site-blocking process:

(a) Rights holders collect evidence of structurally-infringing sites and services to demonstrate copyright infringement as their primary purpose;

(b) If possible, notification is given to the site or service owner or operator with a short deadline for response;

(c) Rights holders file a legal action in court or an application with the relevant government administrative authority;

(d) Evidence is submitted to the court or administrative authority;

(e) An oral hearing is sometimes conducted in court cases with the participation of the ISPs and plaintiff rights holders; site operators are permitted to participate if they choose to do so;

(f) A court or administrative authority hands down the ruling or order and decides whether the ISP is responsible for the technical implementation costs of the blocking order;

(g) Blockings are implemented by ISPs; and

(h) An appeal option exists to enable the blocked websites or services, ISPs and, often, users of the relevant site or services to challenge the order.

62. Appeal or review options are usually available, regardless of whether the site blocking is carried out via court orders or administrative decisions. Importantly, appeals must not have a delaying effect on the blockings.

63. As summarized by a report published in 2024, “in general, a party seeking to obtain a site-blocking order (usually a rights-holder or organization acting on behalf of a group of rights-holders) has a high burden of proof to show that the site in question is either exclusively or substantially devoted to piracy and that a blocking order is justified. Due process is a key component of site-blocking procedures around the world, with the owners of the sites targeted for blocking provided the opportunity to oppose the proposed orders.”[93]

IV. TECHNICAL MEANS OF SITE BLOCKING

64. This section of the study provides an examination of technical approaches to implementing site blocking and a comparative view of their pros and cons.

[93] IP House, “Overseas and Out of Reach”, September 2024, p.28, https://reports.digitalcitizensalliance.org/ip-house.

A. OVERVIEW OF THE INTERNET

65. From a technical perspective, the Internet is a global system of interconnected computer networks using a widely known, standardized set of rules and protocols called the Transmission Control Protocol/Internet Protocol (TCP/IP) suite (also referred to as a protocol stack). It is a network of networks that consists of millions of private, public, academic, business and government networks of a local and global scope, linked by a broad array of electronic, wireless and optical networking technologies. The TCP/IP suite constitutes the structural foundation on which the Internet is built. The suite operates at four distinct but connected layers: (i) network; (ii) Internet; (iii) transport; and (iv) application.

66. All information sent over the Internet is chopped into small digital “postcards”, also called packets or frames; these packets are called “IP frames”, where IP stands for Internet Protocol. The data produced at the application layer (web browsing data, emails, movies, streaming videos, voice calls or files, etc.) are chopped into small IP frames and reassembled into the format of the original files; any errors or missing frames are re-transmitted. The software that does the disassembly on the sending side and reassembly at the destination is called “TCP” for Transfer Control Protocol and operates at the transport layer. It is able to deposit IP frames for transmission in the same way that we deposit a postcard in a mailbox.

67. The service that sends this frame to the right destination is the IP service, which operates at the Internet layer. It uses a unique address, which is attached to each frame, to assign a destination. That address is known as the IP address and works in the same way that a phone number is used to specify whom we are calling. The transferring of IP frames from one network node to another, thus forming a route to the destination, is performed by IP routers. These are the central office switches of the Internet that switch each frame by its IP address into the port connected to the next node.

B. TECHNICAL SITE-BLOCKING METHODS

68. There are several technical methods to block or restrict access to websites and content on the Internet. This study will examine three of the blocking methods that are most commonly used, notably to block access to specific domains, IP addresses and web pages. These technical blocking methods are:

- Domain Name System[94] (DNS) blocking;
- IP address blocking; and
- Uniform Resource Locator (URL)[95] blocking.

69. The analysis of these site-blocking methods will be carried out in accordance with some of the criteria set out by the Internet Architecture Board of the Internet Engineering Task Force

[94] The DNS is a hierarchical, decentralized naming system for computers, services or other resources connected to the Internet or a private network.

[95] The Uniform Resource Locator (URL) is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

(IETF)[96] in the Internet Draft "Technical Considerations for Internet Service Blocking and Filtering".[97] These criteria are:

- Scope: to evaluate which users are blocked;
- Granularity: to evaluate how specific the blocking method is and how it affects other contents and services;
- Efficacy: to evaluate how difficult it is for piracy operators to avoid the blocking method and for users to bypass the blocking method and access the infringing content;
- Feasibility: to evaluate how difficult and costly it is for ISPs to implement the site-blocking method.

70. With respect to scope, any technical site-blocking method implemented at the ISP level applies only to users of those ISPs subject to the jurisdiction of the authority (court or administrative agency) competent to issue the blocking order. Its application is therefore limited to a country's national borders and it does not affect the rest of the Internet or apply to other countries. To be fully effective at the national level, every ISP operating within the country's borders needs to comply with the blocking order. The scope evaluation is therefore the same for all of the blocking methods analyzed below.

a) Domain Name System (DNS) blocking method

- DNS blocking is by far the technical method most widely used by ISPs to carry out site blocking. The DNS provides and ensures the correspondence between a unique numeric IP address, such as 192.0.32.10 - effective but not so easy to manage - and a human-readable logical name[98] (www.example.com), providing a "phonebook-like" lookup of Internet resources.

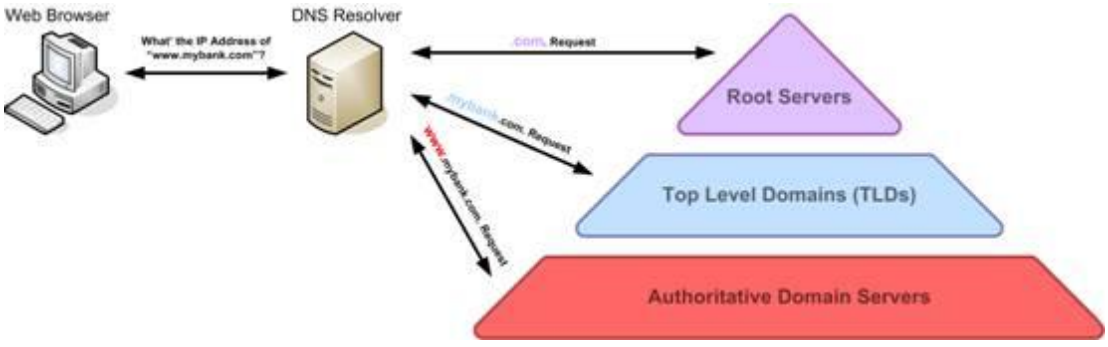


Figure 2 - DNS lookup and hierarchy

[96] IETF is an open standards organization, founded in 1986, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite. The technical work of the IETF is carried out by Working Groups (WGs), the primary mechanism for the development of IETF specifications and guidelines, many of which are intended to set standards or recommendations. Among the various types of working documents produced by the IETF WGs are the so-called 'Internet Drafts", which address specific topics in the areas of competence of each WG. More information is available at: https://www.ietf.org.

[97] IETF, "*Technical Considerations for Internet Service Blocking and Filtering draft-iab-filtering-considerations*", available at: http://tools.ietf.org/html/draft-iab-filtering-considerations-04#section-4.1.

[98] A logical name is a human-readable name used to identify a resource on the Internet, i.e., its domain name (e.g., google.com).

71. The DNS namespace is a hierarchical, inverted tree structure, with a unique root and a large number of sub-trees called domains, further divided into subdomains.

72. The DNS Resolver is like a librarian who is asked to find a particular book somewhere in a library, while the Root nameserver can be thought of as an index in a library that indicates different racks of books, typically serving as a reference for other more specific locations. Following this analogy, the Top-Level Domain (TLD) nameserver can be thought of as a specific rack of books in a library and the Authoritative nameserver – the last stop – as a pointer on the specific rack of books, in which a specific book title can then be transferred to the first requestor, the librarian.

73. Usually, a user's computer, cell phone or other Internet-connected device will use the DNS Resolver of the user's ISP when seeking to connect to a particular website. An ISP is therefore always able to operate a block via its own DNS Resolver. When an ISP blocks a domain name via DNS blocking, then if a client of the ISP types in the domain name on their device, the DNS Resolver refuses to undertake the query, reporting the domain as non-existent (NXDOMAIN or DNS_PROBE_FINISHED_NXDOMAIN). This kind of response to a domain name means than all subdomains that may exist under the particular domain name will also be blocked (e.g., if www.example.com is blocked, then www.legal.example.com will also be blocked).[99]

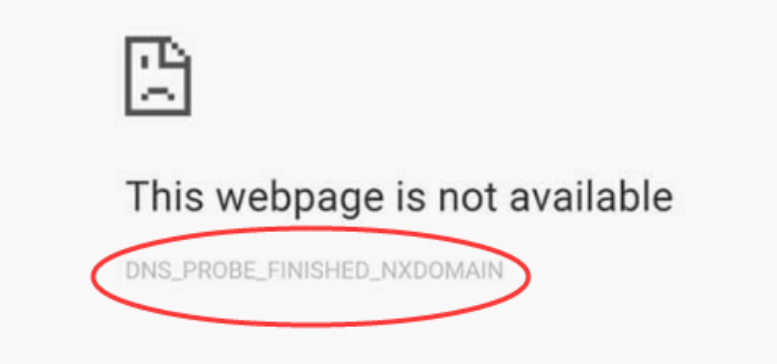


Figure 3 - ISP DNS Block - NXDOMAIN

74. The ISP might also redirect users towards a landing page that displays information about the reason for blocking or other useful information.[100]

Granularity

75. DNS blocking permits granularity because it can apply to subdomains as well as domains. For example, if a piracy website is located at "guilty.example.com" and a legal website is located at "innocent.example.com", then blocking the domain "example.com" will block access to both subdomains. This can be resolved, however, by applying the DNS block to the subdomain "guilty.example.com" only. As long as a domain or subdomain is primarily devoted to illegal copyright infringement, then DNS blocking has the granularity to apply effectively.

99 See Internet Engineering Task Force Request for Comments: 8020 (IETF RFC 8020).
100 Discussed in Section IV.B.

Efficacy

76. The DNS blocking method works with respect to all different types of websites engaged in copyright piracy, including sites that host content, sites that index Bit Torrent or similar files, sites that link to infringing content hosted on other sites and servers, and sites involved in the illegal streaming of live content. This is because, irrespective of the type of infringement in which the operator is engaged, the operator will rely on a domain name for users to locate the piracy operator's site or service. Piracy operators will often acquire multiple domain names in different TLDs.[101] By switching to new domain names, they can avoid the DNS blocking method. This can be addressed, however, by dynamic site-blocking orders that readily and quickly permit these new domain names to be added to the blocking order.

77. DNS resolvers are always included by ISPs as part of the service they offer their customers for Internet access. However, other services that operate on the Internet (e.g., Google, OpenDNS, Mozilla, etc.) also provide DNS resolvers. While such providers of DNS resolvers may be subject to site-blocking orders related to DNS blocking,[102] more often — at least to date — the blocking orders are issued only with respect to ISPs. Therefore, users have the possibility of accessing illegal content blocked by ISPs using DNS blocking by changing the configuration of their devices and by choosing a different DNS resolver, often located outside the national territory in which the blocking order was issued. In addition, users can employ Virtual Private Networks (VPNs)[103] to avoid the blocks implemented by their ISPs. Despite these possibilities for circumvention, studies have indicated that DNS blocking is effective in reducing traffic to piracy sites and online services (see Section II above). This is particularly the case when the DNS blocking orders are issued with respect to a substantial number of popular piracy websites and where such orders are dynamic so as to quickly block the new domains to which the piracy websites migrate.

Feasibility

78. The costs and technical equipment requirements of implementing DNS blocking method are negligible. In addition, this blocking method can be implemented very quickly with minimal engineering/human time and resources. The low cost and ease of implementation, combined with the high degree of efficacy and the ability to target subdomains in terms of granularity, is why DNS blocking is the method currently used most frequently by ISPs for site blocking.

- IP Address blocking method

79. The IP address is a unique address that a device (such as a computer) or hosting server uses to identify itself and communicate with other devices and servers in the IP network. It is analogous to a street address that helps to identify and reach a place in the real world. It can be public or private, static or dynamic, and consists of a 32-bit number written in "dotted decimal" notation, namely four (4) sets of numbers separated by periods.

---

101 There are over 1,500 TLDs, including generic TLDs (e.g., .com, .net., .org, .info) and country code TLDs (e.g., .de for Germany, .cn for China, .br for Brazil).

102 See, for example, Court of Appeal (Oberlandesgericht) of Cologne of November 9, 2020, 6 U 32/20, para. 93; District Court of Hamburg of May 12, 2021, 310 O 99/21.

103 VPNs, or Virtual Private Networks, change a user's IP address to make it appear as if they are browsing the Internet from a different location. Using a VPN can facilitate users' ability to circumvent site blocking by their ISP and allow them to access websites that are blocked in their country.

80. A typical example of an IP address, according the IPv4 standard,[104] is:

64.233.167.99
(www.google.it)

81. Every Internet communication flows from its source to its destination through a series of routers, and across multiple networks in the form of packets containing source and destination IP addresses, as well as the "payload", the substantive content of the communication.

82. An IP address may be associated with a single website hosted on a dedicated server or with multiple websites that use shared hosting services on a server.[105] This is akin to a street address, which might represent a single residence, or an apartment building comprised of multiple residences.

83. ISPs can readily block IP addresses on their networks. Packets sent to or received from the targeted IP address are immediately blocked and will not be able to reach their destination, preventing communication irrespective of the domain name(s) related to the IP address. If multiple websites share an IP address, including ones engaged in either legal activity or in illegal activity, then blocking the IP address will prevent access to all of the websites using that IP address.

Granularity

84. IP address blocking carries the risk of "over-blocking". This is because this method will cut off access to all websites and content that share hosting services on the server to which the IP address is assigned.[106] If the IP address is used exclusively by the copyright-infringing website or service, then this is not a problem. Because popular piracy websites generate a lot of web traffic, they typically rely on a hosting server (and often multiple hosting servers) exclusively for their operations and therefore use one or more dedicated IP addresses. However, if the piracy website uses a shared hosting plan or service, then legitimate websites and domains may also be hosted at the same IP address as the piracy website. IP address blocking will then cause a problem because the method will not be sufficiently targeted and its impact will be overly broad. This can be a particular issue with respect to hosting providers that offer hosting solutions to their customers, providing them with web storage for personal pages, blogs or other services that use shared servers and IP addresses. IP address blocking can also pose challenges with respect to certain online services provided by companies such as Cloudflare. Cloudflare, Inc., is an American Internet intermediary and website-security company that provides content-delivery-network services, Internet security and distributed domain-name-server services. Cloudflare acts as a reverse proxy for websites,[107] sitting between the website's hosting provider and the visitor to that website. Blocking the reverse proxy IP address

---

104 Internet Protocol version 4 (IPv4) is the fourth version of the IP. It is one of the core protocols of standards-based working methods on the Internet and other packet-switched networks. IPv4 was the first version deployed for production in the ARPANET in 1983. It still routes most Internet traffic today, despite the ongoing deployment of a successor protocol, IPv6. IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980). IPv4 uses a 32-bit address space, which limits the number of unique hosts to 4,294,967,296 (232), but large blocks are reserved for special networking methods.

105 Cory, Nigel, "How Website Blocking Is Curbing Digital Piracy Without 'Breaking the Internet", Information Technology & Innovation Foundation, August 2016.

106 For more information about shared IP addresses and dedicated IP addresses, see Kaspersky, "What is an IP Address—Definition and Explanation", https://usa.kaspersky.com/resource-center/definitions/what-is-an-ip-address.

107 A reverse proxy is a type of proxy server that retrieves resources on behalf of a client from one or more servers. These resources are then returned to the client, appearing as if they originated from the proxy server itself. Unlike a forward proxy, which is an intermediary for its associated clients to contact any server, a reverse proxy is an intermediary for its associated servers to be contacted by any client. In other words, a proxy acts on behalf of the client(s), while a reverse proxy acts on behalf of the server(s).

could result in blocking all websites that make use of Cloudflare, not just particular websites devoted to copyright infringement.

85. In addition, popular piracy websites or piracy websites that offer a large amount of content will make use of many servers (each with a different IP address) in order to address caching needs and to increase the speed with which the content is delivered to the users. In such circumstances, it is important to identify all of the IP addresses used in order for the site blocking to be effective.

86. If a website or service dedicated to copyright infringement makes use of one or more dedicated IP addresses, then IP address blocking works well and efficiently. As with DNS blocking, piracy operators can change the IP address they use to avoid orders blocking IP addresses. This can be tackled, however, through dynamic site-blocking orders that readily and quickly enable the new IP address to be added to the blocking order. Furthermore, it is more costly and time-consuming for piracy operators to obtain alternative servers with new IP addresses and make them functional than it is for them to obtain new domain names that simply point or redirect to the already existing servers. Users themselves can circumvent the blockade by routing their traffic away from the blocks through the use of VPNs. However, alternative DNS resolvers do not facilitate the circumvention of IP-address blocks.

Feasibility

87. IP-address blocking is straightforward for ISPs to implement. Costs and deployment difficulties may be considered low owing to the structure of ISP networks.

URL blocking method

88. A URL is a reference to any resource accessible somewhere on the Internet.

89. A typical example of a URL is: http://somewhere.net/products/index, where “http://” is the access method, “somewhere.net” the domain name and “/products/index” is the identity of the resource. A URL is more specific than a domain name because it can refer to a single file or webpage located on a website. This structure is very similar to that of the paths to folders and files on one’s regular computer: there is a root folder (directory), inside which there are other folders, which, in turn, may contain other folders and files.

Granularity

90. URL blocking is the most granular blocking method. It can make a distinction between specific web pages or files existing under the same domain name and hosted at the same IP address. For example, www.example.com/IllegalContent may be blocked, while www.example.com/LegalContent may be allowed.

Efficacy

91. The granularity of URL blocking can render it fairly ineffective when addressing websites with large amounts of copyright-infringing content. This is because each piece of content or link to an infringing piece of content will have its own URL. A URL block will therefore need to be implemented for every infringing piece of content or link on the website. Moreover, it is very easy for the operators of piracy websites or services to change the URLs for the content on their websites and thereby avoid the impact of the site-blocking order without having to secure either

a new domain name or a new server or IP address. In addition, users can employ VPNs or anonymous web proxies to bypass the filters that the ISP uses to carry out URL blocking.

Feasibility

92. URL blocking is more costly and demanding for ISPs to implement than DNS or IP-address blocking. This is particularly true if hundreds or thousands of URL blocks are required in order to block access to all of the infringing content on a commercial-scale piracy website. Moreover, as explained by a service offering different types of filtering and blocking, because URL blocking "is more granular than DNS [blocking], it may also require more maintenance and customization. Additionally, it needs to be implemented separately for each application protocol. By contrast, DNS [blocking] is protocol-agnostic; once turned on, it applies to all types of web traffic."[108]

93. **Conclusion**: While DNS blocking is the most frequently employed technical measure for site blocking, it is not uncommon for site-blocking orders against major piracy websites or services to include both DNS blocks and IP address blocks.

V. SITE BLOCKING AND POTENTIAL CONFLICTS WITH OTHER RIGHTS

94. Questions have been raised about site blocking with respect to its impact on other fundamental rights, such as free speech and the right to conduct a business. The Internet Society, for example, has raised concerns that site blocking can restrict free and open communications, intrude on privacy rights and encourage a lack of transparency with respect to the Internet.[109] The Internet Society has stated that "[i]mplemented without due regards to notions such as necessity and proportionality, content blocking has the potential to cause significant collateral damage, restriction of free and open communications, and put limits on the rights of individuals."[110]

95. Courts around the world have taken these concerns seriously and addressed them in their decisions to issue site-blocking orders. A common theme is the principle of proportionality. Courts will consider, for example, whether they have the ability to address a copyright infringement more directly by ordering the site operator to stop the infringing activity or order the hosting provider to take down the website. However, these parties are usually based in foreign countries and beyond the jurisdictional reach of the particular court considering the appropriate remedy. The court will therefore usually consider site blocking to be a reasonable and proportional remedy because the ISPs subject to the court's jurisdiction are best placed to reduce the infringements.

96. The proportionality principle, however, is also considered with respect to balancing the rights of IP holders to enforce their rights with those of Internet users and businesses providing Internet access and infrastructure. These include issues such as impacts on speech and freedom to communicate and the costs and burdens involved in implementing site-blocking orders.

97. In the UPC Telekabel decision, for example, the CJEU recognized the need to strike a fair balance between fundamental rights, such as the protection of IPRs, the freedom of information

---

108 Cloudflare, "What is URL filtering?", https://www.cloudflare.com/learning/access-management/what-is-url-filtering/.

109 Internet Society, "Internet Society Perspectives on Internet Content Blocking: An Overview", March 2017, https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/.

110 *Ibid*.

of Internet users and the freedom to conduct a business. In applying this balancing test and examining whether site blocking constitutes a proportional remedy, the CJEU found that if the site-blocking measures are targeted at the infringing activity and do not impact the ISP users' ability to lawfully access information, then it satisfies the rights-balancing test and is a proportional remedy. With respect to the right to conduct a business, the CJEU acknowledged that implementing site blocking will impose costs on ISPs. The CJEU concluded, however, that the costs of implementing site blocking do "not seem to infringe the very substance of the freedom of an Internet service provider ... to conduct a business."[111]

98. The High Court of Delhi also addressed many of these issues in the *UTV Software v. 1337X.to* case. With respect to the right of communication and the goal of an open Internet, the Court concluded that "just as supporting bans on the import of ivory or cross-border human trafficking does not make one a protectionist, supporting website blocking for sites dedicated to piracy does not make one an opponent of a free and open Internet. Consequently, this Court is of the opinion that advocating limits on accessing illegal content online does not violate open Internet principles."[112] In terms of imposing the costs of implementing site-blocking orders on ISPs, the Court held that "website blocking costs look reasonable, especially when compared against total ISP operating revenue and investments." After examining court decisions in other countries, the High Court of Delhi concluded that "website blocking has emerged as one of the most successful, cost effective and proportionate means to address this issue [of piracy of copyrighted works online.]"

99. Another concern that has been raised about site-blocking orders is whether they are compatible with the principle of due process. This been addressed both in statutory provisions and in case law. For example, Section 115A of the Australian Copyright Act, which provides a statutory basis for site-blocking orders, requires that the copyright holder seeking a site-blocking order "must notify the person who operates the online location" that is claimed to be engaging in the infringement at issue. The Act further provides that such a notification requirement may be dispensed with "if the Court is satisfied that the owner of the copyright is unable, despite reasonable efforts, to determine the identity or address of the person who operates the online location, or to send notices to that person." This requirement to notify the operator of the infringing website or online service when feasible is fairly standard in site-blocking procedures for copyright infringement around the world. Furthermore, operators of websites or online locations subject to site-blocking action are normally granted the right to participate in proceedings to object to or challenge the order. Finally, ISPs, operators of blocked websites and even users in certain jurisdictions have the ability to appeal a site-blocking order. For example, the CJEU noted in the UPC Telekabel site-blocking decision that to ensure due process and that a fair balance of rights is maintained, "national procedural rules must provide a possibility for Internet users to assert their rights before the court once the implementing measures taken by the Internet service provider are known."[113]

100. A study in 2022 concluded that, "as implemented to date, website blocking is a fair, effective, and proportionate tool to target sites involved in the mass, illegal dissemination of copyrighted content and that it does not undermine human rights, free speech, or net neutrality."[114]

---

111 Judgment of March 27, 2014, UPC Telekabel, C-314/12, EU:C:2014:192, para. 51 (https://curia.europa.eu/juris/document/document.jsf?docid=149924&doclang=EN).

112 *Utv Software Communication Ltd. and Ors v. 1337X.To and Ors*, High Court of Delhi at New Delhi, April 10, 2019, para. 55, https://indiankanoon.org/doc/47479491/.

113 Judgment of March 27, 2014, UPC Telekabel, C-314/12, EU:C:2014:192, para. 57, https://curia.europa.eu/juris/document/document.jsf?docid=149924&doclang=EN.

114 Cory, Nigel, "A Decade After SOPA/PIPA, It's Time to Revisit Website Blocking", Information Technology & Innovation Foundation, January 2022, https://itif.org/publications/2022/01/26/decade-after-sopa-pipa-time-to-revisit-website-blocking/.

VI. PRACTICAL CHALLENGES AND MAINTAINING THE EFFECTIVENESS OF SITE BLOCKING

101. Digital and online environments create difficult and ever-evolving challenges in the fight against copyright piracy. No single strategy or method can defeat or eliminate copyright piracy. As recently noted in one study, "just as no alarm system or door lock will ever work 'perfectly' to keep out all invaders, no technology will be able to completely eliminate online piracy of copyrighted works."[115]

102. Both copyright owners and governments need to embrace an array of different strategies to address online copyright piracy conducted on a commercial scale. These include:

(a) Providing consumer-friendly legal alternatives for accessing content;

(b) Restricting the financial gains to pirate operators, often referred to as the "follow-the-money" approach that encourages online advertisers and payment processors to cut off their services to piracy websites;[116]

(c) Criminally prosecuting pirate operators;

(d) Providing efficient legal paths for effective orders to stop Internet intermediaries and online service providers of all kinds from providing their services and resources to pirate operators; and

(e) Making voluntary arrangements whereby copyright owners alert Internet intermediaries and service providers (including online advertisers and payment processers) to the existence of copyright piracy websites and the relevant companies stop providing their services to those websites.[117]

103. The above strategies are illustrative and do not constitute an exhaustive list. Given the ability of pirate operators to reside anywhere and to readily use Internet-related resources from multiple jurisdictions worldwide to reach a global audience, multiple strategies and tools must be deployed.

104. Section II above indicates that site blocking has proven to be an effective tool in the fight against commercial-scale online copyright piracy. Nonetheless, in order to maintain its efficacy, site blocking has had to evolve to address two key challenges: (i) circumvention efforts by pirate operators and, to a lesser extent, the users of piracy websites, to avoid the access restrictions, and (ii) the evolution of technical means by which content is distributed online (e.g. downloading from a single source, peer-to-peer file sharing, streaming).

---

115 Mossoff, Adam, "Congress Should Protect the Rights of American Creators with Site-Blocking Legislation", The Heritage Foundation, February 2024, https://www.heritage.org/crime-and-justice/report/congress-should-protect-the-rights-american-creators-site-blocking

116 See for example the Government of Canada's Final Report "Examination of the 'follow-the-money approach' to copyright piracy reduction", April 2016, https://www.canada.ca/en/canadian-heritage/e/copyright-policy-publications/follow-money-piracy.html

117 Trusted notifier/flagger arrangements are an example. For an explanation of such arrangements with respect to domain name service providers, see Marks, Dean and Nordemann, Jan, "The Role of the Domain Name System and its Operators in Online Copyright Enforcement", WIPO Advisory Committee on Enforcement, WIPO/ACE/15/7 August 2022 pp. 42-42 and Annex 1, https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ace_15/wipo_ace_15_7.pdf For an example of voluntary efforts on the part of online advertisers, see the Trustworthy Accountability Group https://www.tagtoday.net/

A. CIRCUMVENTION CHALLENGES

105. To avoid the impact of site-blocking orders, pirate operators shift their websites or online services to new domain names,[118] different servers with different IP addresses, and/or new websites that simply result in redirection to the original blocked website. These tactics involve what are often referred to as "mirror" or "redirect" sites. To address this challenge, countries around the world have evolved their site-blocking regimes to allow for dynamic blocking injunctions.[119] A dynamic blocking injunction permits new domain names, IP addresses and/or URLs that represent the same website or service for which a site-blocking injunction has been issued to be added to the blocking order without a new full judicial or administrative proceeding. Dynamic blocking injunctions thus provide an efficient and cost-effective way to "keep up" with the pirate operators. As noted in an in-depth study on dynamic blocking injunctions undertaken by the European Union Intellectual Property Office (EUIPO), dynamic injunctions allow "rights holders to respond to efforts made by the website operators to circumvent the orders by changing the location of the target website."[120] The EUIPO study also notes that dynamic blocking orders can address the concern of potential over-blocking by requiring rights holders "to notify the ISPs of IP addresses, URLs and/or domain names that should no longer be blocked, for example, where an IP address/URL which has been notified for blocking ceases to be a location whose sole or predominant purpose is to enable or facilitate access to a target website."[121] The European Commission has issued guidance supporting dynamic blocking injunctions as a forward-looking remedy "that can be an effective means to prevent the continuation of an IPR infringement."[122]

106. The typical scenario for mirror sites is illustrated below with the example of the illegal service "subsmovies". It was included in a Danish blocking order in 2017, with the website address "subsmovies.com" at the time. The figure illustrates how, after the blocking of the original domain, a mirror site, "subsmovies.me", was created. The mirror site increased in popularity until blocked and replaced by a further mirror site at "subsmovies.nl" that in turn was superseded by a third mirror, "subsmovies.nz", which was eventually also blocked. The dotted, vertical lines represent the blocking of the sites. This example shows why it is crucial that mirror sites are quickly detected and blocked in order to have an optimal effect, and why dynamic site blocking is so important to ensure efficacy.

---

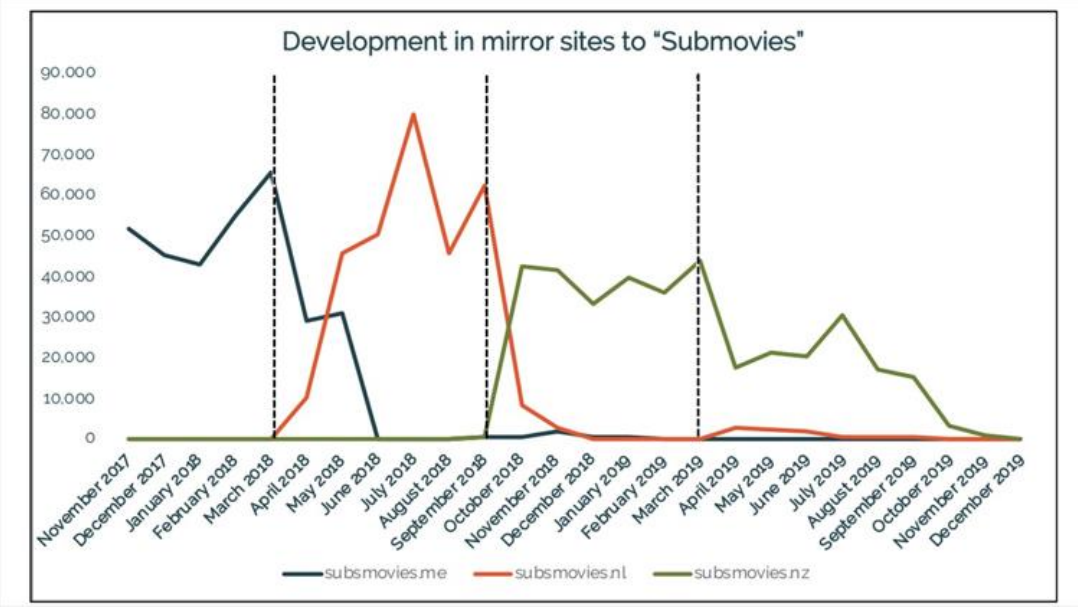
118 For example, the Pirate Bay website made use of multiple different top-level domains such as ".mn", ".gd", ".vg" and ".la" to avoid blocking orders in the earlier years of site blocking. Protalinski, Emil "The Pirate Bay is not down: Domain redirect problem has an easy fix", Venture Beat, May 2015, https://venturebeat.com/media/the-pirate-bay-is-not-down-domain-redirect-problem-has-an-easy-fix/

119 According to a 2022 study the following countries have adopted dynamic site blocking: Australia, Belgium, Brazil, Denmark, France, India, Indonesia, Ireland, Israel, Italy, Malaysia, Netherlands, Portugal, Russia, Singapore, Spain, Sweden, Thailand and the United Kingdom. Appendix, Cory, Nigel, "A Decade After SOPA/PIPA, It's Time to Revisit Website Blocking", Information Technology & Innovation Foundation, January 2022 https://itif.org/publications/2022/01/26/decade-after-sopa-pipa-time-to-revisit-website-blocking/

120 EUIPO, "Study on Dynamic Blocking Injunctions in the European Union", March 2021, https://www.euipo.europa.eu/en/publications/dynamic-blocking-injunctions-in-the-eu

121 Ibid at p. 37.

122 European Commission, Communication to the European Parliament, the Council and the European Economic and Social Committee, Guidance on certain aspects of Directive 2004/48/EC, Com/2017/708/final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0708



107. Recently, some countries have expanded dynamic blocking injunctions to reach beyond new domain names or host locations of the same piracy website that was subject to the original blocking order. This expansion is called "pirate brand site blocking". Under this concept, websites that provide users with a similar service and set of infringing content as the original target website may also be included in the blocking injunction, even if the website operator is different from that of the original target website. In the context of pirate brand site blocking, rights holders notify the ISPs of the new piracy websites that use the same name or substantially similar name to that of the target website and provide the same or a substantially similar layout and functionality as the original target website. Then the domain names and/or IP addresses of these new websites are added to the blocking order. With pirate brand site blocking, rights holders can provide a notification for the blocking not only of the mirror and redirect sites of the original target website, but also any structurally infringing websites operating in the same fashion and using the same brand name (e.g. 123movies, 123moviesfree, 123series) without having to prove that it is connected to the main target website.

108. Both the United Kingdom and Spain have adopted pirate brand site blocking. For example, in 2022 the Barcelona Commercial Court in Spain ruled the following as part of a site-blocking order:

"I order the defendant companies to block or prevent, through such technical means and mechanisms as they should consider most effective to terminate or reduce significantly, in a real and effective manner, access by their clients from Spanish territory to the websites that make use of the brands HDFULL or GNULA, including the websites with the following current names of the main domain: gnula.cc, gnula2.co, hd-full.com, hdfull.so".

109. The blocking order also includes other domains, subdomains and IP addresses that (either on the website itself or in the domain name) **use any of the HDFULL or GNULA brands mentioned above to identify structurally infringing services used to access audiovisual works to which the plaintiffs hold the reproduction, distribution and public communication rights, without their consent**; and must inform the court and the plaintiff immediately once such technical measures have been adopted and of the steps taken to carry out such blocking orders.

110. The plaintiff rights holders will be responsible for supervising, detecting and monitoring the possible appearance in the market of such domains, subdomains and IP addresses that use (either in the website itself or in the domain name) any of the aforementioned HDFULL or GNULA brands to identify structurally infringing services for access to audiovisual works to which the plaintiffs hold the rights of reproduction, distribution and public communication, without their consent. The defendants are released from any obligation of control in this regard.

111. In the event that plaintiffs detect such domains, subdomains and IP addresses that use any of the aforementioned HDFULL or GNULA brands to identify structurally infringing services for access to audiovisual works to which plaintiffs hold the reproduction, distribution and public communication rights, without their consent, they shall notify defendants, and shall duly identify such domains, subdomains and IP addresses.

112. Upon receipt of such notice, the defendants shall voluntarily extend the blocking to such domains, subdomains and IP addresses that use any of the aforementioned HDFULL or GNULA brands to identify services that enable access to audiovisual works to which the plaintiffs hold reproduction, distribution and public communication rights, without their consent."

113. The defendants shall be required to block access to such domains, subdomains and IP addresses only when the plaintiffs provide (i) evidence of the use of the pirate HDFULL or GNULA brands (either on the website itself or in the domain name) and (ii) confirmation of the structurally infringing nature of the website."[123]

114. The above quoted language from the Spanish court decision sets forth a number of fundamental principles that are typical of both dynamic and pirate brand site-blocking orders. These include the following:

(a) It is the responsibility of the rights holders to monitor the emergence of new websites that should be blocked under dynamic and pirate brand site-blocking orders. The rights holders need to identify the new websites, their domain names, relevant subdomains and IP addresses. They also need to affirm that the new websites: (i) are structurally infringing services, and (ii) infringe on the rights holders' copyrights. In addition, the rights holders need to collect evidence supporting such affirmations.

(b) For dynamic and pirate brand site-blocking orders, the rights holders can often notify the ISPs directly of the new websites that satisfy the conditions set forth in the order, without having to first notify or solicit approval from the court or administrative authority. Those notices will need to be accompanied by the affirmations and evidence as set forth in paragraph 1 above.

(c) Upon receipt of compliant notices from the rights holders, the ISPs must block the additional websites.

(d) Often courts or administrative authorities let the ISPs decide which technical mechanism or combination of mechanisms (e.g. DNS blocking, IP address, URL blocking) to employ to accomplish the blocking. This can be the case whether the blocking order is static, dynamic or for a pirate brand.

115. In one pirate brand site-blocking decision issued in the United Kingdom, the court made clear that it is the responsibility of the rights holders to try to avoid "over-blocking", particularly with respect to IP addresses. In its order, the court directed that the rights holders must notify the ISPs if "any Target Website where the server of the notified IP address hosts a site or sites

[123] Juzgado de lo Mercantil No. 6 de Barcelona, February 21, 2022, Universal City Studios, et. al. v. Vodafone Espana, et. al., Case No. 0801947120218009156, Proceeding 744/2021-S, unpublished.

that are not part of a Target Website and one or more of the site or sites that are not part of the Target Website ceases to carry out unlawful activity. In this case, the Respondents [ISPs] shall not be required to block that IP address."[124]

116. The advantages of pirate brand site-blocking are clear: (i) they increase the locations that can be notified to ISPs to block under an order without having to return to court or the relevant administrative authority, thereby reducing the number of legal actions/applications that need to be filed by rights holders; (ii) they provide a more effective and faster means of dealing with circumvention efforts by pirates; and (iii) they significantly increase the ongoing efficacy of site-blocking orders.

117. Dynamic and pirate brand site blocking represent worthy and useful advances in the field of site blocking. However, they do not address user circumvention efforts that involve the active choice of individuals to use VPNs or alternative DNS resolvers. This is because site-blocking injunctions normally only apply to ISPs, and ISPs do not have control over VPNs or alternative DNS resolvers. However, some courts have sought to address this circumvention problem by ordering DNS resolvers that are independent of ISPs, but which offer their services to consumers in the country of the court's jurisdiction to also block access to the identified piracy website.[125] With respect to circumvention of site-blocking orders by VPNs, French courts have ordered search engines to de-index the target websites from their search results and to do so on a dynamic basis that addresses new or copycat versions of the websites based on the brand name.[126] Recently, an Italian court held Cloudflare, a content delivery network that can also be used to quickly change domain name extensions, liable for copyright infringement by providing its services to a website operator whose website had been blocked by the Italian Communications Regulatory Authority (AGCOM). The court ordered Cloudflare to cease providing its services to the website and set a fine of 1,000 euros a day for non-compliance with its order.[127] In September 2024, the Lisbon Intellectual Property Court in Portugal issued a ruling against Google Portugal for its failure to implement blocks against the website "EZTV" along with 500 related subdomains by its Google DNS service, which can be used as an alternative DNS resolver to circumvent DNS blocks implemented by ISPs. The Court rejected Google's arguments that it lacks the technical capability to block the domains since the public DNS service is managed by Google Ireland. Rather, the Court held that Google Portugal acted as an intermediary, and that Google's alternative DNS service, available to users in Portugal, circumvents existing site-blocking orders, facilitating access to illegal content.[128] By imposing obligations on alternative DNS resolvers, content delivery networks and other service providers that are independent of ISP access providers, courts are increasing the efficacy of site-blocking orders.

118. Beginning in 2023, both Argentina and Italy have also taken substantive steps forward to include a broad range of Internet intermediaries and service providers within the scope of orders related to site blocking, with a view to increasing their effectiveness. As noted in Section III above, as part of a site-blocking order, a court in Argentina ordered Google to disable a pirate

---

124 Columbia Pictures and British Telecommunications, High Court of Justice, Business and Property Courts of England and Wales, IL-2022-000055, July 15, 2022, (https://www.bailii.org/ew/cases/EWHC/Ch/2021/2799.html)

125 See, for example, the German court decisions: Court of Appeal (Oberlandesgericht) Cologne of November 2020, 6 U 32/20 para. 93; District Court of Hamburg of May 12, 2021, 310 O 99/21. See also Marks, Dean and Nordemann, Jan, "The Role of the Domain Name System and its Operators in Online Copyright Enforcement", WIPO Advisory Committee on Enforcement WIPO/ACE/15/7, August 2022, pp. 27–29 https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ace_15/wipo_ace_15_7.pdf

126 See discussion of French court decisions in EUIPO "Study on Dynamic Blocking Injunctions in the European Union", March 2021, p.76, https://www.euipo.europa.eu/en/publications/dynamic-blocking-injunctions-in-the-eu

127 See https://www.broadbandtvnews.com/2024/11/22/mediaset-secures-copyright-infringement-judgement-against-cloudflare/

128 See: https://www.shine.cn/biz/company/2409186481/ and https://www.theportugalnews.com/news/2024-09-18/google-portugal-ordered-to-block-pirate-site/92193#:~:text=Google%20Portugal%20has%20been%20ordered,from%20the%20company%20told%20Lusa

app that could be installed on its Android operating system. As explained in Annex 2, Italy has recently permitted orders to be issued against a broad range of Internet intermediaries in conjunction with site-blocking orders issued against ISPs by AGCOM.

B. TECHNICAL EVOLUTION CHALLENGES

119. The technical means by which copyrighted content can be distributed over the Internet have evolved and continue to change and develop. Digital versions of music, books, films and television programs used to be available only for download on static websites. Subsequently, peer-to-peer file-sharing technology such as BitTorrent emerged, enabling users to obtain and download content quickly from multiple computers and without reliance on a central server.[129] With this evolution in technology, indexing and linking websites such as The Pirate Bay emerged, facilitating massive online copyright piracy. Streaming technology then evolved, which allowed users to view or listen to content over the Internet without downloading it. Similarly, Internet Protocol television (IPTV) is an online service that delivers live broadcasts and on-demand videos over the Internet.

120. While all of these technological developments can and do support legal activity, they can also can be readily abused to facilitate online copyright piracy on a damaging commercial scale.[130] To keep pace with the rapidly developing technology and the parallel evolution of illegal markets, site blocking needs to be developed and refined on a legal, procedural and technical basis. From downloads via file-sharing technology to streaming and stream-ripping services, and the movement from centralized services via websites to decentralized services via apps or media boxes, these developments have all occurred within a few years and all present challenges. Therefore, site blocking must be continuously developed in order to remain effective and address the evolving online technologies and innovations.

21. With respect to the emergence of peer-to-peer file sharing, courts and administrative agencies around the world have expanded the concept of what constitutes a copyright piracy website for which a site-blocking remedy is appropriate. Multiple courts have ruled that piracy websites include indexing and linking sites whose predominate purpose is to enable users to download or access content that infringes copyright, even when such sites themselves do not host the content. Furthermore, even when the links to the infringing content are placed on the site by the users rather than the site operator, if the primary purpose or effect of the site is to facilitate copyright infringement, then it will still qualify as a copyright piracy website (see, for example, the discussion in Section III above concerning the CJEU decision about The Pirate Bay indexing website).

121. In recent years, unauthorized streaming of live events (such as sporting event broadcasts) and live streaming of subscription cable channels, television broadcasts and other services have become a major target of piracy operators.[131] These services are sometimes referred to as illicit Internet Protocol TV services or illicit IPTV. Essentially, pirates steal or rip the signal from legal cable boxes and legal streaming services and then share it with their customers via an app or media box preloaded with specific software, such as Kodi boxes.[132] These pirate live-streaming services are often more difficult to block, as the operators do not need to rely on a stable website known to their customers, but rather can use multiple servers to send the digital signals to their apps or media boxes. Rights holders are normally responsible for identifying the

---

129 For a more detailed explanation as to how BitTorrent functions, see Hoffman, Chris, “How Does BitTorrent Work?”, How-To Geek, September 2016, https://www.howtogeek.com/141257/htg-explains-how-does-bittorrent-work/

130 For a more detailed discussion of how copyright piracy websites and services are currently operating and evolving, see: IP House “Overseas and Out of Reach”, September 2024, https://reports.digitalcitizensalliance.org/ip-house

131 For a more in-depth explanation of various pirate IPTV and live-streaming services, see: Ibid.

132 For more information about Kodi boxes, see: https://www.makeuseof.com/tag/kodi-boxes-legal-own-one/

relevant domain names and/or the IP addresses for the servers involved in live streaming. The site-blocking orders are then based on DNS and/or IP address blocks. With respect to live events such as sporting events, to be effective the blocking must be implemented very quickly, at the time the event is occurring and being streamed. In order to accomplish this, rights holders must seek and obtain the legal order from the relevant court or administrative authority prior to the live event, with the flexibility of notifying the ISPs as soon as the relevant IP addresses are identified by the rights holders associated with the illegal IPTV streams.

122. Countries including Ireland, Italy, the Netherlands, Portugal, Spain and the United Kingdom have issued live blocking orders for ISPs to block access to the IP addresses of servers dedicated to streaming the live content.

C. MEASURES TO SUPPORT THE EFFECTIVENESS OF SITE BLOCKING

123. The implementation of dynamic, pirate brand and live orders, and the expansion of orders related to site blocking for other Internet intermediaries, increase and support the effectiveness of site blocking. Nonetheless, other measures can also be adopted, including voluntary agreements, information-sharing and consumer education and awareness. Some of these additional measures have already been adopted in certain countries to increase the efficacy of their site-blocking regimes.

124. In Denmark, the ISPs and rights holders have entered into a voluntary Code of Conduct with respect to site blocking.[133] If one ISP in Denmark is ordered to block an illegal website, the other ISPs operating in Denmark will also block the website. Further, the Code of Conduct permits rights holders and ISPs to collaborate on the appropriate blocking techniques and methods to be used for the particular website or service that infringes copyright. This voluntary "one-stop-shop" approach is coordinated on behalf of rights holders by the RettighedsAlliancen (Danish Rights Alliance). It has resulted in the pragmatic handling of the many site-blocking injunctions issued by Danish courts, and reflects the positive and practical cooperation between the rights holders and ISPs in Denmark. It also increases the effectiveness of site blocking by ensuring the compliance of all ISPs with the blocking orders. In addition, the collaboration has led to the rapid implementation of dynamic blocking to address redirect and mirror sites. The voluntary cooperation is also beneficial to ISPs, as they can avoid litigation costs related to site-blocking lawsuits. Furthermore, this cooperative approach is also helpful in the dialogue with government authorities that will often endorse a less intrusive self-regulatory approach, rather than hard regulation that may be viewed as more burdensome by the ISPs.

125. A study commissioned by the European Parliament on Cross Border Enforcement of Intellectual Property Rights in EU highlighted the Danish voluntary Code of Conduct with respect to site blocking and noted that it is "highly efficient and effective due in large part to its streamlined procedure, even considering the fact that a court order is a prerequisite for website blocking. Rights holders also report that their ability to submit blocking applications with respect to many different categories of infringing websites (e.g. stream ripping, BitTorrent indexing sites and linking sites) provides an additional advantage of the Danish system over that of other [EU member States]."[134]

126. Portugal's site-blocking regime also incorporates a voluntary agreement. A Memorandum of Understanding was agreed upon by ISPs and rights holder associations in 2015 to facilitate a

---

133 Denmark: Code of Conduct on website blocking, https://www.teleindu.dk/wp-content/uploads/2014/10/TI-code-of-conduct-blokeringer.pdf

134 European Parliament, "Cross Border Enforcement of Intellectual Property Rights in EU", December 2021 at p.39, https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2021)703387

process for blocking piracy websites without the need for a court order (see Annex 2 for more details).

127. In 2021, a voluntary arrangement in Germany was made between ISPs and rights holders called the Clearingstelle Urheberrecht in Internet (CUII). The CUII provides a procedure for site-blocking orders against websites that structurally infringe copyright without the need for a court order. An application is made by rights holders to the CUII committee and, if the committee decides unanimously that the website(s) should be blocked, the ISPs implement the block, unless a concern is expressed by the government Federal Network Agency.[135]

128. Ideally, voluntary arrangements, including Codes of Conduct, should enable and set forth:

- **One-stop implementation**: this means a blocking order is accepted and implemented by all ISPs in the country, even if all the ISPs are not specified in the order.

- **Timeframes**: it should be agreed that implementation will take place within a specific time period, e.g. a maximum of three days. It should be taken into account that different kinds of content have different sensibility levels in relation to blocking. For instance, websites or servers offering live content need to be blocked immediately, whereas websites offering content that has already been released commercially, such as television programs or recorded music, can be blocked within a longer period of time, i.e. a few days.

- **Notification to site operators**: the operators of websites that are subject to site-blocking orders should be notified, but only when this is practically possible. If there is contact information on the site, this can be used for notification. It must not be overly burdensome to make notifications, as such a requirement can undermine the effectiveness of the system. On the other hand, the operators should have the option to defend their interests if they choose to do so.

- **Implementation process**: it should be agreed that all ISPs – or the most important ones, measured by coverage – will receive and implement the site-blocking orders in their technical systems through an automatic process. This can be done through an application programming interface for a database listing infringing websites that are subject to blocking orders. Alternatively, stakeholders can agree to deliver a list every week, which ISPs implement on weekly basis, unless urgent blocking is required, e.g. blocking of live content.

- **Handling of mirror and redirect sites**: the criteria for identifying mirror and redirect sites, the stakeholder responsible for identifying them, and the process for their blocking should all be specified. In addition, if either the national law permits or the ISPs and rights holders agree to pirate brand blocking, then a similar process should also be specified for reliable and efficient implementation.

- **Notice to end-users**: when end-users deliberately or accidentally attempt to access an illegal website or service that is subject to blocking, they should be informed about the blocking and why it has been implemented. This can be done in different ways, but a standardized message posted by all ISPs on a standardized landing page that the users see is preferable. As described later in this Section, the optimal landing page will help guide users to legal services to access the desired content.

135 Ibid.

- **Other Internet intermediaries**: if other Internet intermediaries such as search engines, domain name service providers, alternative DNS resolvers, and proxy servers are willing to stop providing search results and services on a voluntary basis with respect to piracy websites that have been subject to site-blocking orders, this will serve to increase the efficacy of such orders.

129. Information-sharing is another method of supporting site blocking, and courts will sometimes reference site-blocking orders from other countries with respect to the same website that is under their consideration. For example, in a site-blocking order that applied in part to numerous websites and domain names of The Pirate Bay (TPB), the Federal Court of Australia issued the following statement: "As I have also mentioned, blocking orders have already been made in relation to many of the TPB sites in other jurisdictions. I am satisfied that it is appropriate to grant an injunction under s 115 in respect of each of the active TPB sites."[136]

130. WIPO has also facilitated information-sharing concerning websites that structurally infringe copyright through its WIPO ALERT database.[137] WIPO ALERT permits WIPO Member States to submit to a database the details of websites that they have determined to deliberately infringe copyright. Many of the participating Member States submit the details of websites that have been subject to site-blocking orders in their countries.[138] Advertisers, advertising agencies and their technical service providers can apply to become authorized users of WIPO ALERT in order to access aggregated lists of websites that infringe copyright from around the world. They can use this information in their automated advertising systems to avoid placing advertisements on such sites. In this way, they can avoid subsidizing copyright infringement and protect their brands from the negative reputational effect of association with illegal activities.

131. Beyond such information sharing, in the European Union suggestions have been made concerning potential cross-border site-blocking orders that provide greater efficiency and wider impact. The European Parliament study "Cross Border Enforcement of Intellectual Property Rights in EU" examined a number of websites that infringe copyright that have been subject to site-blocking orders in multiple EU member States.[139] With respect to the website The Pirate Bay, the study noted multiple legal actions taken against the website between 2006 and 2020 in 15 member States, the majority of which were site-blocking actions. The study included the following questions: "is this multiplication of repetitive legal actions an efficient allocation of private and public money that serves well online copyright enforcement in the Single Digital Market? Is this justified from a public policy perspective? Perhaps, the history of legal actions against TPB suggests that there is an urgent need to facilitate online cross-border enforcement in the EU."[140]

132. For piracy websites that are popular across multiple EU member States, a procedure for achieving cross-border site-blocking orders would relieve the burdens of cost and time to obtain such orders on a State-by-State basis. The European Parliament study further noted that "from a public policy perspective, it is also unsatisfactory that copyright and related rights are mostly enforced in some (mostly larger and/or richer) [member States (MS)] […] [T]he continued availability of infringing websites in some (mostly smaller and/or less wealthy) MS is also unsatisfactory from the perspective of affirming and developing the culture of access to copyright works through legitimate services. Development of pan-EU solutions, permitting rights holders to overcome the limitations of the MS-by-MS approach, would greatly facilitate the

---

136 Roadshow Films v. Telstra Corporation, FCA 1503 (2016), para 98.

137 See: https://www.wipo.int/web/wipo-alert

138 For the various criteria that the participating Member States use to submit websites to WIPO ALERT, see: https://www.wipo.int/web/wipo-alert/operating-procedures

139 European Parliament, "Cross Border Enforcement of Intellectual Property Rights in EU", December 2021, pp. 58–64

140 Ibid at p. 61

establishment of the Digital Single Market as well as ensure the equitable treatment of businesses and citizens regardless of the MS of their residence."[141]

133. Whether or not the European Union will develop a procedure or system for cross-border site-blocking orders with respect to piracy websites that are popular across the EU remains to be seen. The European Parliament study, however, sets forth strong arguments on the benefits of such cross-border enforcement, not only for rights holders, but also for citizens and the economies of all EU member States. Given that piracy websites: (i) frequently deliver malware to their users, causing harm, (ii) result in losses and damages to copyright holders and the creative industries, and (iii) deprive national economies of tax revenues and business income from the legitimate businesses that piracy websites steal from, even countries outside the European Union may wish to consider how to expedite site blocks against websites that have already been subject to blocking orders in other countries.

134. User education is yet another method to support the effectiveness of site blocking. Site blocking in its basic form without a specific landing page will prevent the user from entering the illegal website. However, the user only receives an error message, and therefore may well go to another illegal website in order to find the content they are searching for. This is why it is important for site blocks to lead users to a landing page that informs them of why the website or service is blocked and provides information about where the user can legally find the content that they are searching for. Even though the user may be frustrated about reaching the landing page, this can lead to positive outcomes if the landing page:

- Informs the user that the website or service has been blocked because it is illegal in nature;

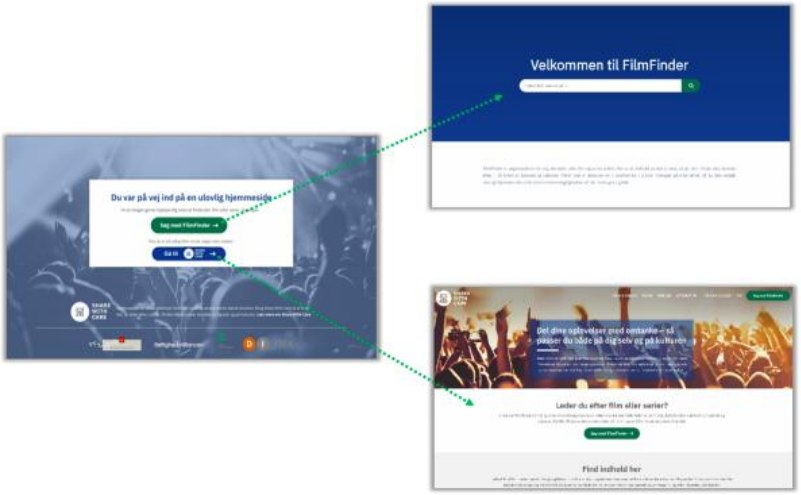
- Warns the user that the illegal website or service may also deliver viruses or malware to the user's computer/cellphone/home entertainment system;

- Guides the user to legal sources for the desired content; and

- Refrains from threatening the user, for example, by referring to the possibility of copyright damage claims against the user.

135. The Danish model, which combines blocking and "nudging" user behavior through standardized landing pages that the user sees when blocking occurs, is probably the most developed one within the European Union. Denmark was the first country to introduce website blocking and was also early in introducing awareness activities in combination with blocking. From the site-blocking landing page, users are directed from the blocking message to a search function called FilmFinder, where they can type the title of a movie or television series and be directed to the legal services offering that content.

141 Ibid at p. 64



136. On average this model prevents 74 per cent of traffic to illegal sites and is used by all Danish ISPs.[142]

VII. CONCLUSION

137. No single solution or "silver bullet" exists to stop online copyright piracy, but site blocking has proven to be an effective tool. Site blocking as a remedy for online copyright piracy is often based on statutory laws that specifically address site blocking or more general statutory language that provides for no-fault injunctive relief against Internet intermediaries for online copyright piracy. However, courts in several countries have adopted site blocking based simply on the already existing general injunctive relief provisions in their copyright laws, both civil and criminal.

138. To sustain its effectiveness, site blocking must continuously evolve to address new kinds of online copyright piracy, such as live events and stream-ripping. In addition, the legal framework for site blocking should allow flexibility to implement dynamic and pirate brand injunctions, as well as live injunctions to address the pirating of live broadcasts and stream ripping. Furthermore, if in conjunction with site-blocking orders courts or administrative agencies order other Internet intermediaries (such as VPNs, DNS resolvers, software system operators, search engines, reverse proxy providers and content delivery networks) to take action to disable piracy websites, pirate apps, pirate services and site-blocking circumvention paths, then this strengthens the impact and effectiveness of the site-blocking orders.

139. In addition, site-blocking regimes that allow for faster and less costly administrative actions, as opposed to lengthy litigations before courts, usually deliver greater efficacy. A well-functioning site-blocking system that involves cooperation between relevant stakeholders (such as Codes of Conduct and voluntary agreements among rights holders and ISPs) and/or automated processes, such as Italy's Piracy Shield platform,[143] further increases the efficiency and effectiveness of a site-blocking regime. Voluntary cooperation also assists in generating insights into circumvention efforts by pirate operators and into user behavior. Finally, site-blocking regimes that embrace and implement consumer education messaging and provide

142 See https://rettighedsalliancen.com/share-with-care/

143 See B. Terraciano, "The Role of AGCOM in Protecting Copyright Online: Tackling Live Event Piracy", WIPO/ACE/17xx

information about legal alternatives for accessing content increase user awareness of how to embrace legal content services and avoid illegal ones.

140. With respect to online piracy websites and services that have wide appeal across many countries, it remains to be seen whether a more dedicated information-sharing system will emerge that: (i) provides details of the sites that are useful for implementing blocking injunctions, and (ii) lists the countries in which such sites have already been blocked. If such a reliable and comprehensive system were to exist, then it would be up to a country's courts, administrative agency and/or voluntary arrangement between rights holders and ISPs to decide whether and how to use such information to expedite their own blocking of such sites. In addition, with respect to regions such as the European Union with a level of legal harmonization among their member States, cross-border site-blocking injunctions may eventually be adopted.

[Annex 1 follows]

ANNEX 1: THE PIRATE BAY

The Pirate Bay is an illustrative example of how both civil and criminal copyright enforcement remedies do not always lead to the shutdown of online copyright piracy websites and services. Launched in Sweden in 2003, The Pirate Bay is a BitTorrent indexing website that enables users who have downloaded the BitTorrent software to search for and download content via torrent links, which the website distributes and indexes in a readily searchable manner. The torrent links themselves are uploaded to The Pirate Bay by its users. This technology makes content distribution very easy and fast. The Pirate Bay is used to distribute music, movies, television programs, video games, and software,[144] the overwhelming majority of which is made available without the authorization of the relevant copyright owners.

In 2006, Swedish law enforcement agents conducted a raid in several different locations and seized 186 servers of The Pirate Bay and shut the website down. However, after just three days the website was up and running again online via a backup that had been created by one of the co-founders of The Pirate Bay prior to the raid.[145]

In 2007, a criminal prosecution in Sweden was initiated in the District Court against four co-founders of The Pirate Bay for complicity in committing crimes in violation of the Copyright Act. The co-founders were found guilty and sentenced to one-year prison sentences and held jointly liable for copyright infringement damages of approximately 3.3 million euros. The co-founders appealed their criminal convictions, but they were upheld in 2010 by the Court of Appeal. The Court of Appeal reduced the prison sentences and increased the joint liability for damages to approximately 5 million euros. Subsequently, in 2012, two of the convicted co-founders filed an appeal with the European Court of Human Rights and argued that their criminal convictions were inconsistent with Article 10 of the European Convention on Human Rights concerning the right to receive and impart information. The European Court of Human Rights unanimously rejected their application and found the criminal convictions compatible with the Convention.[146] Nevertheless, according to at least one report the co-founders never paid the damages that were assessed.[147]

Meanwhile, civil litigation resulted in decisions requiring hosting providers to shut down servers hosting The Pirate Bay and domain service providers to suspend various domain names of The Pirate Bay. In addition, site-blocking legal actions were brought in at least 12 EU member States to block access to The Pirate Bay[148] as well as in other countries around the world. In December 2014, another raid was made by Swedish police who seized servers, computer equipment and other equipment.[149]

Today, almost 19 years since the initial law enforcement raid and despite multiple civil litigations as well as criminal prosecutions, The Pirate Bay is still up and running. Although the CJEU confirmed that The Pirate Bay is engaged in illegal copyright infringement, it is still popular and

---

144 See: https://en.wikipedia.org/wiki/The_Pirate_Bay

145 See: https://torrentfreak.com/the-pirate-bay-turns-15-years-old-180810/

146 *Neii and Sunde Kolmisoppi v. Sweden*, No. 40397/12 ECHR (Fifth Section), 19/02/2013, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-117513%22]}

147 See: https://hackread.com/pirate-bay-founders-to-pay-e405000-to-record-labels/#:~:text=In%202009%2C%20Fredrik%20Neij%2C%20Gottfrid,did%20serve%20time%20in%20prison

148 "Cross Border Enforcement of Intellectual Property Rights in EU", European Parliament, December 2021 pp. 60–61

149 See: https://en.wikipedia.org/wiki/The_Pirate_Bay

receives millions of visits.[150] This illustrates how both traditional civil and criminal copyright remedies, as well as more innovative remedies such as site blocking, cannot eliminate online piracy. Given the global nature of the Internet, as long as intermediaries, online advertisers and payment providers in various countries are willing to provide their services to copyright pirates, the problem of online copyright piracy will persist.

[Annex 2 follows]

150 See: https://www.similarweb.com/website/thepiratebay.org/#overview

ANNEX 2: CASE EXAMPLES OF ADMINISTRATIVE SITE BLOCKING

Italy, Portugal and the Republic of Korea have been selected for discussion of their administrative site-blocking procedures as they have been in operation for a number of years and have evolved and expanded over time. These nations were chosen based on a review of the challenges faced and strategies used to address site blocking, reflecting the global diversity in legal structures, enforcement mechanisms, and cultural contexts.

A. ITALY

The Italian Communications Regulatory Authority (AGCOM) was established in 1997 to regulate telecommunications, the press, and the audiovisual and publishing sectors. Since December 2013, AGCOM has been granted powers to settle administrative online copyright enforcement issues and to undertake educational and awareness-raising activities aimed at preventing piracy.

According to the Regulation on the Protection of Copyright on Electronic Communications Networks and Procedures for the Implementation thereof pursuant to Legislative Decree No. 70 of April 9, 2003 (approved by Resolution No. 680/13/CONS of December 12, 2013, Italy),[151] only rights holders or their representatives may lodge a complaint and start proceedings. All other interested parties (e.g. ISPs and website owners) become involved later in proceedings by exercising their right of defense and submitting relevant documentation.

When assessing a case of actual online copyright piracy, AGCOM may adopt several measures, depending on the location of the server hosting the website and its content:

- if the server is located in Italy – AGCOM's home jurisdiction – the authority may order the hosting provider to remove the infringing content from the website; and
- if the server is located abroad, since it is not possible to order the selective removal of illegal content, AGCOM may order the ISPs established in Italy to disable access to the website by blocking the DNS resolution or the IP address.

Regular proceedings are completed within 35 working days but are fast-tracked whenever infringements occur on a massive scale (e.g. a large number of copyrighted works, websites that are entirely devoted to piracy and/or are capable of seriously harming rights holders (for instance, when new and important content is hosted on website). In these cases, AGCOM issues an order within 12 working days.

The Regulation also establishes some indicators (art. 9 c.3) in order to define the severity and scale of the infringement when evaluating the use of fast-track proceedings.

The main factors to be considered are:

- a) circumstances under which, in relation to the same object and following a previous request, the Authority has already deemed there to be a violation of copyright or related rights pursuant to Article 8, paragraph 2;
- b) the significance of the quantity of digital works alleged to have been disseminated in violation of copyright or related rights;
- c) the timing of when the digital work was placed on the market;
- d) the economic value of the violated rights and the extent of the damage caused by the alleged violation of copyright or related rights;

[151] Available in the original language at: https://www.agcom.it/documents/10179/23527627/Allegato+2-8-2021+1627897969927/a6fe9eb8-9a81-44ef-8e9b-652cfe6c75a8?version=1.0

- e) the promotion or encouragement, even indirectly, of the use of digital works disseminated in violation of the Copyright Law;
- f) the misleading nature of the message, such as to induce the user to mistakenly believe that it is a legitimate activity;
- g) the provision of information regarding the technical methods for accessing digital works disseminated illegally; and
- h) the purpose of profit in the illegal offering of digital works, which can also be deduced from the onerous nature of their use or from the dissemination of advertising messages.

In 2018, Italy amended the Regulation, introducing new provisions on two types of fast-track proceedings.

First, the amendments have clarified how to handle websites that, even if blocked in the past, frequently reappear with different DNS names (so-called “mirror sites”). If AGCOM has already issued an order against that website, a rights holder may initiate fast-track proceedings by notifying the new infringement. Within three days, if there is confirmation of the recurrence of the infringement, the newly reported website is included in the list of infringing websites that access providers must block. In establishing whether there is a recurrent infringement, AGCOM evaluates elements such as the similarity of the domain name, matching IP address, references on the website to the same social network profiles or groups, the identity of the domain name registrant and the layout and graphics that feature on the website. With this amendment, Italy and AGCOM have embraced dynamic site blocking as described in Section VI of the study.

Second, an applicant may seek interim measures based on the risk of imminent, serious and irreparable harm related to the illegal consumption of online audiovisual contents (for example, during their release in cinemas). In such cases, AGCOM needs to take measures within three days of receiving the application. If a precautionary order is issued, the hosting or access providers must comply with it within two days. The addressee of the precautionary order may lodge an appeal within five days of receiving the order. If not appealed, the order remains in force and becomes final.

In both cases, AGCOM has the authority to adopt preventive measures and update the list of domain names used by infringing websites.

Since 2014, AGCOM has received more than 5,000 (5,096 as of October 31, 2024) complaints of copyright infringement, primarily concerning massive copyright violations. Most of the complaints concerned copyright infringements in the online environment, while only a few (18) were lodged for infringements on more traditional audiovisual or radio media services. In terms of the types of copyrighted works infringed upon, complaints primarily referred to audiovisual (films, television series, live football games) and musical content and, to a lesser extent, to images and editorial content such as that which is found in newspapers and journals.

The primary focus of fast-track proceedings under the Regulation has been related to illegal audiovisual and music consumption, which has resulted in a large number of proceedings being brought against cases of massive infringement.

The effectiveness of the Regulation has resulted in a significant amount of voluntarily removed illegal content, with around 28 per cent of proceedings being closed without a final order issued by AGCOM. However, despite these good results, 1,367 DNS website-blocking orders have been adopted under the Regulation since 2014, due to massive copyright infringements, and the majority of these websites were hosted on servers located outside of Italy.

In 2023, Law No. 93/2023 expanded the capacity of AGCOM to combat online piracy, introducing "live injunctions", which enable the rapid blocking of sites and services linked to the illegal online streaming of broadcasts of live events protected by copyright or related rights.

In addition, Law No. 93/2023 permits AGCOM to issue orders not only to ISPs, but also to other Internet intermediaries such as search engines, VPN providers, alternative DNS resolver providers, and reverse proxy server providers. The Law provides that both ISPs and other Internet intermediaries involved in facilitating access to the illegal websites or services must quickly execute blocking orders and orders to suspend their services or functions with respect to the identified piracy websites or illegal online services that infringe copyright.[152]

Furthermore, Law No. 93/2023 required the creation of a machine-to-machine platform for expediting the submission of complaints by verified and credentialed rights holders and compliance with blocking orders by ISPs and other Internet intermediaries. This platform, called Piracy Shield, has been operational since early 2024. As a result, blocks facilitated through Piracy Shield are realized within 30 minutes of notification. Since February 1, 2024, more than 26,000 domains and 7,000 IP addresses have been blocked through the use of Piracy Shield.[153]

B. PORTUGAL

The first instance of site blocking in Portugal (relating to The Pirate Bay website) took place by way of a civil court order in February 2015.[154] However, since this initial order, the country has moved towards an administrative procedure.[155]

Administrative blocking was introduced in July 2015, following a voluntary memorandum of understanding between the Inspectorate General of Cultural Affairs (IGAC), which reports to the Ministry of Culture, the Portuguese Association of Telecommunications Operators (APRITEL) and the rights holders' association MAPINET (a cross-sector anti-piracy organization).[156]

According to the memorandum, MAPINET should first notify the website or platform of the existence of content that infringes copyright and request its removal. If the platform responds negatively or fails to respond, MAPINET can refer the matter to IGAC. As a requirement, rights holders must demonstrate that the website provides access to at least 500 protected works, or that two thirds (66 per cent) of the content hosted on the website infringes copyright. IGAC carries out the necessary checks within a few days (48 hours on average), and then instructs ISPs to place a DNS block on the site within 48 hours. This is done twice a month according to a schedule set out in the memorandum, so that ISPs are required to mobilize their resources and teams at regular, pre-set intervals. The costs of implementing the blocks are borne by the service providers.[157] A study of Portugal's site-blocking regime that examined data up to

---

152 For further details and information, see: B. Terraciano, "The Role of AGCOM in Protecting Copyright Online: Tackling Live Event Piracy", WIPO/ACE/17/xx

153 For more information about Piracy Shield, see Ibid.

154 See: https://www.lexology.com/library/detail.aspx?g=63981942-6078-415c-919e-aa1a12addfb5

155 Information from the French authority HADOPI, which in its report "Anti-piracy strategies of cultural and sports content" has summarized and compared different national approaches to the fight against Internet IP infringement with a particular focus on blockings. Some of these findings are presented in the following: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.hadopi.fr%2Fsites%2Fdefault%2Ffiles%2Fsites%2Fdefault%2Ffiles%2Fckeditor_files%2FHADOPI_COLLOQUE_INTERNATIONAL_RAPPORT_VEILLE_ENG_HD.pdfg=AOvVaw1TnU7ZMsYRt_Jl63XYuGRd&ust=1598210109653000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCKD2huzCr-sCFQAAAAAdAAAAABAD

156 High Authority for the dissemination of works and the protection of rights on the Internet (HADOPI). Anti-Piracy Strategies of Cultural and Sports Content – 2019 International Survey, https://rettighedsalliancen.dk/wp-content/uploads/2020/05/HADOPI-rapport.pdf

157 Ibid.

October 2016 revealed that, in this relatively short period of time, the site blocks reduced the usage in Portugal of the websites targeted by the blocking orders by 69.7 per cent.[158]

Since early 2019, an addendum to the memorandum of understanding was made to facilitate temporary DNS blocking of live streaming of sporting events. Thus, since January 2019, it is possible to extend the administrative DNS blocking system to sites providing unauthorized access to sports content and to implement "live blocking" measures during the televised broadcasting of sporting events.[159] Dozens of live-streaming websites were blocked in the first few weeks of operation of this new system.[160]

In 2022, Law No. 82/2021 entered into force in Portugal, adding regulatory authority to the voluntary administrative process that has been in place since 2015. It establishes the authority of IGAC to legally determine the removal or prevention of access to copyrighted content made available illegally. It also sets forth obligations for hosting providers, search engines and other Internet intermediaries to take action to address infringing content and piracy websites and services.[161]

C. REPUBLIC OF KOREA

The Republic of Korea has introduced an administrative blocking system, which mainly targets foreign websites. In the first step of the procedure, the Korea Copyright Protection Agency (KCOPA) verifies the content of the site concerned. If more than 70 per cent of the content is illegal, it requests that the site be blocked. The Ministry of Culture, Sport and Tourism (the Ministry) then instructs the Korea Communications Standards Commission to proceed with blocking the site. As for sites with local domain names, they may have their domain name withdrawn.

In the Republic of Korea, platforms are regarded as a specific type of technical intermediary, a list of which is drawn up by the Ministry. They are under obligation to acquire content recognition or search filtering tools (enabling keyword filtering, for example). Platforms must use these technologies upon the request of rights holders. Otherwise, they incur a fine and, if fined more than three times, they receive a commercial penalty and may even be banned from operating in the Republic of Korea.

In addition, the Republic of Korea has a "graduated response" system that targets both platforms that enable the illegal downloading of content and end-users who download and/or share illegal content online. Under this system, when these illegal activities are identified – including by rights holders – the KCOPA works with the Ministry and warnings are sent out. If the illegal activity continues, then platforms and users can be penalized.

In addition, the country implements actions to raise awareness and promote the consumption of authorized content. The 2015 Clean Site initiative (now known as Copyright OK) led to the creation of a dedicated website administered by the public authorities, which certifies the legality of websites providing creative content. Certified sites can then display the Copyright OK logo on their pages.

---

158 See: https://www.incoproip.com/wp-content/uploads/2020/02/Site-Blocking-and-Piracy-Landscape-in-Portugal-May-2017.pdf

159 See: https://www.technadu.com/portugal-extending-piracy-blocking-to-live-sports/55280/

160 High Authority for the dissemination of works and the protection of rights on the Internet (HADOPI). Anti-Piracy Strategies concerning Cultural and Sports Content in France and Abroad, 2019–2020 International Survey, https://www.hadopi.fr/sites/default/files/sites/default/files/ckeditor_files/2021_06_01_Rapport_veille_internationale_2019_2020_vENG.pdf

161 For more details about Portugal's Law No. 82/2021, see: https://www.vda.pt/pt/publicacoes/insights/new-rules-in-portugal-for-removing-and-preventing-access-to-copyrighted-content-in-the-digital/24554/

[Annex 3 follows]

ANNEX 3
COUNTRIES ACTIVELY USING WEBSITE BLOCKING
(As of January 2022)

With the kind authorization of Mr. Nigel Cory, the following annex is a reproduction of the Appendix "Countries Actively Using Website Blocking" from his Information Technology and Innovation Foundation (ITIF) paper, "A Decade After SOPA/PIPA, It's Time to Revisit Website Blocking"[162], with the following information, as of January 2022:

"*In total, at least 48 countries allow website blocking for copyright infringement. Of those, 33 (not counting the EU) actively allow rightsholders to use website-blocking injunctions for copyright infringement. At least another 12 countries (e.g., Bulgaria, Croatia, Cyprus, the Czech Republic, Estonia, Hungary, Liechtenstein, Luxembourg, Malta, Poland, Slovakia, and Slovenia.) have laws that technically allow website blocking, but they aren't in use as of yet. Some countries (e.g., Vietnam and Saudi Arabia) have blocked infringing copyright sites on an ad hoc basis, as they do not have a dedicated legal or administration framework for website blocking.*

The following list provides a snapshot of how different countries use website blocking for copyright enforcement.

***Argentina** [static and dynamic]. In 2014, Argentina became the first Latin American country to block The Pirate Bay on copyright grounds.[163] The legal framework for the injunction came from Argentina's Copyright Law.[164] Upon urging from the Cámara Argentina de Productores de Fonogramas (CAPIF), an Argentinian music industry group, the Argentine National Communications Commission ordered ISPs to block access to multiple domain names and IP addresses related to the site. In all, 12 domains and 256 IP addresses had to be blocked. However, this appears to have been a one-time sting, and Argentina has not routinely issued website-blocking injunctions since.*

***Australia** [static and dynamic]. Australian courts have allowed website blocking since 2016.[165] However, at the end of 2018, blocking efforts significantly increased after a review of the blocking policy.[166] In the largest wave of blocking in the country's history, 233 domains associated with 99 websites were blocklisted.[167] As part of the reforms made by the review, copyright owners and ISPs can privately agree to extend an injunction to include any new websites that host the same infringing material without having to go back to court for a new injunction.[168] Likewise, search engines such as Google and Bing are held responsible for*

---

162 www2.itif.org/2022-revisiting-website-blocking.pdf

163 Andy Maxwell, "The Pirate Bay Now Blocked in Argentina," Torrent Freak, July 1, 2014, https://torrentfreak.com/the-pirate-bay-now-blocked-in-argentina-140701/

164 "Argentina: Law No. 11.723 of September 28, 1933, on Legal Intellectual Property Regime (Copyright Law, as amended up to Law No. 26.570 of November 25, 2009)," WIPO IP Portal, https://wipolex.wipo.int/en/text/225488.

165 Malcolm Burrows, "s115A Copyright Act – infringement outside Australia," Dundas Lawyers blog, July 9, 2020, https://www.dundaslawyers.com.au/s115a-copyright-act-infringement-outside-australia/.

166 "Review of the Copyright Online Infringement Amendment," Australia's Department of Infrastructure, Transport, Regional Development, and Communication, https://www.infrastructure.gov.au/have-your-say/review-copyright-online-infringement-amendment

167 Motion Picture Association, "Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior: December 2018" (study, January 2020), https://www.mpa-apac.org/wp-content/uploads/2020/02/Australia-Site-Blocking-Summary-January-2020.pdf.

168 Joanne Gray, "Site-blocking under review: Who determines Australia's internet experience?," Digital Social Contract blog, September 7, 2020, https://digitalsocialcontract.net/site-blocking-under-review-who-determines-australias-internet-experience-b26bb50f2bb3

removing links to blocked sites, as well as their mirrors and proxies.[169] Australia has instituted a rigorous regime for website blocking that increased traffic to legal streaming sites by 5 percent from 2018 to 2020.[170]

***Austria** [static]. Following the CJEU's 2014 ruling in Telekabel v. Constantin Film that permitted orders to ISPs to block certain websites, Austria began a website-blocking program of its own.[171] This ability was later confirmed by the Austrian Supreme Court in 2017 after a lengthy legal battle with The Pirate Bay.[172] ISPs have requested the creation of an "independent judicial body" to confirm in advance the legality of any blocking while ensuring that a minimum of time and resources are expended on the blocking process, though this has not yet materialized.[173]*

***Belgium** [static and dynamic]. In 2013, the Belgian Supreme Court ruled in a long-lasting legal battle between rights holders and The Pirate Bay. confirming the lawfulness of generic IP blocking injunction orders against all national ISPs.[174] Since then, Belgium has been able to institute a policy of website blocking, blocking 33 websites and 450 domains on copyright grounds in 2018 alone.[175]*

***Brazil** [static and dynamic]. Brazil's 2019 Operation 404 campaign was the country's first instance of website blocking.[176] The campaign has been repeated twice more in the following years, with Operation 404 #3 occurring in July 2021. Each wave blocked hundreds of domains associated with piracy sites. Whether these operations will continue, and Brazil will standardize a system for getting injunctions, is yet to be seen.*

***Canada** [static]. In May of 2021, a Canadian appeals court upheld the country's first-ever website-blocking framework.[177] This decision allowed ISPs to block access to the IPTV provider GoldTV for providing pirated content. The decision drew from the Canadian Copyright Act as well as the Telecommunications Act.[178] The decision by the Court, while welcome, does not obviate the need for an efficient and specific amendment to the Copyright Act to create a "no fault" mechanism for obtaining blocking orders such as what exists in the European Union,*

---

169 Emma Woollacott, "Australia Tightens Online Piracy Laws," Forbes, November 29, 2018, https://www.forbes.com/sites/emmawoollacott/2018/11/29/australia-tightens-online-piracy-laws/?sh=708832f33d12.

170 Motion Picture Association, "Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior: December 2018."

171 . "Web-blocking in Austria – law with the law taken out," EDRi blog, October 22, 2014, https://edri.org/our-work/web-blocking-austria-law-with-the-law-taken-out/.

172 Andy Maxwell, "The Pirate Bay & 1337x Must Be Blocked, Austrian Supreme Court Rules," TorrentFreak, November 14, 2017, https://torrentfreak.com/the-pirate-bay-1337x-must-be-blocked-austrian-supreme-court-rules-171014/.

173 Andy Maxwell, "Austrian Telecoms Regulator Rejects "Informal" Pirate Site Blocks," Torrent Freak, January 18, 2019, https://torrentfreak.com/austrian-telecoms-regulator-rejects-informal-pirate-site-blocks-190118/.

174 Patrick Van Eecke and Alexis Fierens, "In Pirate Bay Case, Belgian Supreme Court Confirms Lawfulness of Generic IP Blocking Injunctions," lexGO.be blog, January 13, 2014, https://www.lexgo.be/en/papers/ip-it-telecom/it-law/in-pirate-bay-case-belgian-supreme-court-confirms-lawfulness-of-generic-ip-blocking-injunctions,83933.html.

175 Robert Briel, "Belgian ISPs agree to block 450 'pirate' domains," BroadbandTV News, May 7, 2018, https://www.broadbandtvnews.com/2018/05/07/belgian-isps-agree-to-block-450-pirate-domains/.

176 Ernesto Van der Sar, "Brazil's Anti-Piracy 'Operation 404' Leads to Arrests, Shutdowns, and Site Blocking," Torrent Freak, July 12, 2021, https://torrentfreak.com/brazils-anti-piracy-operation-404-leads-to-arrests-shutdowns-and-site-blocking-210712/.

177 Barry Sookman, "Blocking orders available in Canada rules Court of Appeal in GoldTV case," Barry Sookman blog, May 27, 2021, https://www.barrysookman.com/2021/05/27/blocking-orders-available-in-canada-rules-court-of-appeal-in-goldtv-case/.

178 "Canada's Copyright Act (1985)," Justice Laws Websitehttps://laws-lois.justice.gc.ca/eng/acts/C-42/Index.html; "Canada's Telecommunications Act (1993)," https://laws.justice.gc.ca/eng/acts/T-3.4/.

Singapore, and Australia. This is being studied by the Canadian Government in its current consultation on copyright reform for online intermediaries.[179]

***Colombia** [static]. In August 2021, Colombia's National Copyright Directorate (Direccion Nacional de Derecho de Autor, DNDA) granted its first blocking injunction against IPTV Colombia Premium, a distributor that violated copyright by broadcasting content from different programmers without permission.*[180]

***Denmark** [static and dynamic]. The Pirate Bay was first blocked in Denmark back in 2008.*[181] *Since that early adoption of the practice, website blocking has expanded to the point where 141 piracy sites were blocked in 2019 alone.*[182] *This increasing pressure on piracy saw visits to pirate sites drop 40 percent from 2018 to 2019. However, this impressive statistic could in part be caused by consumers finding new ways to access the sites rather than through local ISPs, namely through VPNs or pirated content on YouTube/Facebook.*

***Ecuador** [static]. Ecuador's National Service for Intellectual Rights (Servicio Nacional de Derechos Intelectuales, or SENADI) created a site-blocking framework that has proven effective in its initial actions against copyright-infringing sites, including piracy sites retransmitting unauthorized audio and video signals of DIRECTV Ecuador and its national league of professional soccer (LALIGA). The framework is based on legislation (the Organic Code on the Social Economy of Knowledge, Creativity and Innovation).*[183]

***European Union** [static, dynamic, and live]. As detailed in this report, EU courts have ruled on the side of website blocking multiple times in the past decade. First in the 2014 Telekabel v. Constantin Film decision, the CJEU ruled that ISPs can be ordered to block access by customers to websites that make available infringing content. Later in 2017, the European Court of Justice (ECJ) ruled that the notorious The Pirate Bay may be blocked as "the making available and management of an online sharing platform must be considered to be 'an act of communication' for the purposes of the EU Copyright Directive." Additionally, the ECJ has ruled that proof of illegality is unnecessary, as the law exists to prevent infringement as well as to end it.*[184]

***Finland** [static]. Section 60c of the Finnish Copyright Act provides the legal framework for ordering an ISP to block access to infringing sites.*[185] *Another pioneer of website blocking,*

---

179 Barry Sookman, "Blocking orders available in Canada rules Court of Appeal in GoldTV case," Barry Sookman blog, May 27, 2021, https://www.barrysookman.com/2021/05/27/blocking-orders-available-in-canada-rules-court-of-appeal-in-goldtv-case/.

180 "NATIONAL COPYRIGHT DIRECTORATE GRANTS FIRST PRECAUTIONARY MEASURE AGAINSTONLINE PIRACY IN COLOMBIA," Nextv News International, March 15, 2021, https://nextvnews.com/national-copyright-directorate-grants-first-precautionary-measure-against-online-piracy-in-colombia/.

181 "Danish ISP shuts access to file-sharing Pirate Bay," Reuters, February 4, 2008, https://www.reuters.com/article/us-denmark-piratebay/danish-isp-shuts-access-to-file-sharing-pirate-bay-idUKL0480268320080204.

182 Andy Maxwell, "Denmark Blocked 141 Pirate Sites in 2019 But Pirates Are Bypassing The System, "Torrent Freak, May 3, 2020, https://torrentfreak.com/denmark-blocked-141-pirate-sites-in-2019-but-pirates-are-bypassing-the-system-200503/.

183 Ernesto Van der Sar, "Pirate Site Blocking Efforts Expand to Ecuador," Torrent Freak, June 11,2019, https://torrentfreak.com/pirate-site-blocking-efforts-expand-to-ecuador-190611/.

184 "Austrian ISPs ordered to block The Pirate Bay," The Local, July 29, 2014, https://www.thelocal.at/20140729/austrian-isps-ordered-to-block-the-pirate-bay/.

185 "Finland's Copyright Act (404/1961, amendments up to 608/2015), https://www.finlex.fi/en/laki/kaannokset/1961/en19610404.pdf.

Finland first blocked The Pirate Bay in 2011.[186] Since then, there has been little additional action, although in 2018, two injunctions were issued against the torrent sites RARBG and YIFY.[187] Finland's website-blocking policy revolves around ad hoc busts, rather than a robust program of blocking piracy sites as they emerge.

***France** [static and dynamic]. Website blocking is available under a broad implementation of Article 8.3 of the EU Directive, and since 2015, a number of popular BitTorrent and streaming sites have been blocked. in November 2019, the Paris Court ordered ISPs to block of number of notorious cyberlocker sites, including Nippyspace.com. In 2021, France's National Assembly passed a law focused on combatting live sporting event piracy.[188] The law permits rightsholders and broadcasters to obtain immediate injunctions from a judge to block sites illegally streaming a live event. These injunctions apply for 12 months and also cover any "mirror" sites. France also requires search engines to delist pirate sites.[189]*

***Germany**[static]. To facilitate future blocking, in 2021, Germany established a new body (called CUII, as detailed in this report) made up of retired judges with knowledge of German copyright law to review complaints and issue website-blocking orders without needing to go through court.[190] In 2018, a German court issued a provisional injunction that a German ISP (Vodafona Kabel) block access to illegal streaming websiteKinox.to. Even though Kinox.to did not directly distribute the infringing material, it was still considered liable "for a willful and causal breach of duty" to restrict piracy.[191]*

***Greece**[static]. Website blocking is available under the implementation of Article 8.3 of the EU Copyright Directive, and in 2017, Greece adopted legislation introducing an administrative procedure for website blocking. In 2018, Greece issued its first website-blocking orders against blatant piracy sites such as The Pirate Bay.[192] Earlier in 2021, 47 additional domains were added to the blocklist.[193] The Greek procedure does not require court orders; instead, a special commission at the Greek Ministry of Culture and Sports called EDPPI receives and handles requests from rightsholders.*

***Iceland** [static]. In 2015, Iceland issued website-blocking orders against The Pirate Bayand Deildu following a court case the previous year authorized injunctions against intermediaries (e.g., ISPs).[194] The ability to issue these injunctions was later upheld by Iceland's Supreme*

---

186 Ernesto Van der Sar, "Finnish ISP Ordered To Block The Pirate Bay," Torrent Freak, October 26,2011, https://torrentfreak.com/finnish-isp-ordered-to-block-the-pirate-bay-111026/.

187 Ernesto Van der Sar, "Court Orders Finnish ISPs to Block RARBG and YIFY," Torrent Freak, June 8,2018, https://torrentfreak.com/court-orders-finnish-isps-to-block-rarbg-and-yify-180608/.

188 Stuart Thomson, "Rights-holders welcome new French antipiracy law," Digital TV Europe, March 22,2021, https://www.digitaltveurope.com/2021/03/22/rights-holders-welcome-new-french-antipiracy-law/.

189 Thomas Hubert, "French court tackles illegal streaming and download sites," France 24, November 29, 2013, https://www.france24.com/en/20131129-france-court-bans-illegal-video-sites-piracy-downloads-streaming-tv-movies.

190 Chris Cooke, "New organization launched in Germany to allow web-blocking without court orders," CMU, March 15, 2021, https://completemusicupdate.com/article/new-organisation-launched-in-germany-to-allow-web-blocking-without-court-orders/.

191 Jan Willem Aldershoff, "Vodafone forced to block access to illegal video streaming site Kinox.to," myce, February 12, 2018, https://www.myce.com/news/83715-83715/.

192 Ernesto Van der Sar, "Greek ISPs Ordered to Block 38 Domains, Including The Pirate Bay," Torrent Freak, November 9, 2018, https://torrentfreak.com/greek-isps-ordered-to-block-38-domains-including-the-pirate-bay-181109/.

193 Ernesto Van der Sar, "Greece Adds Open Subtitles to Its Pirate Site Blocklist," Torrent Freak, July 21, 2021, https://torrentfreak.com/greece-adds-opensubtitles-to-its-pirate-site-blocklist-210721/.

194 Ernesto Van der Sar, "ISPs Agree to Block The Pirate Bay in Iceland," Torrent Freak, September 17, 2015, https://torrentfreak.com/isps-agree-to-block-the-pirate-bay-in-iceland-150917/; Andy Maxwell, "Freedom-Friendly Iceland Blocks The Pirate Bay," Torrent Freak, October 16, 2014, https://torrentfreak.com/freedom-friendly-iceland-blocks-the-pirate-bay-141016/.

Courtin 2018. Although website blocking has now been established as a legal practice in Iceland, its use is still relatively limited.

***India** [static and dynamic]. In India, websites have been blocked on the basis of copyright infringement using Section 69A of the Information and Technology Act 2000 (as amended in 2008), Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009, and Civil Procedure Rules. In 2019, the Delhi High Court created the mechanisms to allow rightsholders to request dynamic blocking injunctions.[195] These injunctions order ISPs to shut down piracy sites as well as their many "mirror" sites as they pop up. Over 13,000 sites are currently blocked in India following applications to the Calcutta High Court, the Delhi High Court, and, most recently, as a result of a submission to the Maharashtra Digital Crime Unit.*

***Indonesia** [static and dynamic]. In Indonesia, website blocking is available based on government powers, and the procedure was further specified in a copyright amendment act and accompanying regulation adopted in 2015.Beginning in 2019, the Indonesian regulator KOMINFO began a massive wave of website blocking in conjunction with the Video Coalition of Indonesia. Over the course of 2019–2020, over 2,300 piracy sites were blocked, averaging 60 sites blocked every 10 days. Due to these efforts, Indonesia has the lowest levels of illicit streaming device usage in the Asia-Pacific, second only to Singapore. In the year following the start of this "rolling" site blocking, visits to piracy sites fell by 55 percent.[196]*

***Ireland** [static, dynamic, and live]. In 2020, the High Court of Ireland granted UEFA (the governing body of soccer in Europe) a live and dynamic blocking injunction for the duration of the competition season.[197] The Court performed an assessment, finding that (i) the injunction was necessary; ii) the costs involved were not excessive or disproportionate and the order itself should not be unduly complicated; (iii) the cost-sharing proposals were fair and reasonable; (iv) the order respected the fundamental rights of the parties affected, including Internet users; and (v) the duration of the proposed injunction and the provisions for review were reasonable. Furthermore, in 2018, an Irish court granted an injunction to block eight major piracy websites.[198] Those eight websites had received a minimum estimated total of 6,334,215 visits from users in Ireland in October 2017 alone.*

***Israel** [static and dynamic]. In 2019, Israel reformed its copyright law for "indirect infringement" to warrant a website-blocking injunction. Indirect copyright infringement is "making available [pirated material] to the public," so blogs and websites that link to pirated content may also be blocked.[199] The reforms also directly allow courts to order ISPs and other intermediaries to restrict infringing websites, thereby ensuring that website blocking is a viable practice for copyright holders.*

---

195 Nigel Cory, "India and Website Blocking: Courts Allow Dynamic Injunctions to Fight Digital Piracy," Innovation Files blog, May 29, 2019, https://itif.org/publications/2019/05/29/india-and-website-blocking-courts-allow-dynamic-injunctions-fight-digital.

196 "Major Drop in Levels of Streaming Piracy in Indonesia," Satellite Markets and Research, July 15, 2020, http://www.satellitemarkets.com/market-trends/major-drop-levels-streaming-piracy-indonesia.

197 "Union Des Associations Européennes De Football v Eircom Ltd T/A Eir & Ors," High Court of Ireland, September 29, 2020, https://www.bailii.org/ie/cases/IEHC/2020/2020IEHC488.html.

198 John Kennedy, "Movie industry victory as eight piracy sites blocked in Ireland," Silicon Republic, January 16, 2018, https://www.siliconrepublic.com/enterprise/movie-piracy-ireland-legal-action-isps.

199 Yehuda Neubauer, "The new Israeli online anti-piracy copyright reform explained," IAM blog, October 23, 2019, https://www.iam-media.com/new-israeli-online-anti-piracy-copyright-reform-explained ; Karen Elburg , Adar Bengom, and Jenia Melkhior, "Israel: Copyright Law (Amendment No. 5), 2019," Mondaq, January 9, 2019, https://www.mondaq.com/copyright/770562/copyright-law-amendment-no-5-2019.

Italy *[static, dynamic, and live]. In Italy, website blocking is available under the implementation of Article 8.3 of the EU Copyright Directive, criminal law, and a special administrative procedure (AGCOM Regulation) that came into effect at the end of March 2014. Under the regulation, AGCOM (the national communications regulatory authority) has the power to order ISPs to block access to infringing websites upon consideration of a complaint filed by a rightsholder and there is a "fast-track" procedure for websites responsible for massive copyright infringements. In 2020 and 2021, Italian courts granted dynamic blocking injunctions to both Italy's top soccer league (Lega Nazionale Professionisti Serie A) and the Serie BKT (Serie B) competition. The injunctions were for the duration of the season.[200] In 2016, Italian authorities ordered the largest bulk website blocking in the country's history, blocking access to 152 pirated sporting and film sites. According to Italian lawyer Fulvio Sarzana, a legal expert in this area, the order "covers roughly the first four pages of results on Google with regard to the search terms streaming, football, and films."[201]*

Latvia *[static]. In 2019, a new law came into effect that allows the Latvian National Electronic Media Council (NESMI) to issue a website-blocking order to an ISP without the need of a court order.[202] The names and domains of all blocked sites are published on a government website and remain on the national blocklist for six months.*

Lithuania *[static]. In April 2019, amendments to the Lithuanian Copyright Act came into force, which provided for a new administrative procedure allowing rightsholders to obtain a website-blocking order within a month.[203] Rightsholders send a takedown notice to the site operator and the hosting provider, and the operator and/or hosting provider has five days in which to remove the notified content and also ensure the same content is not re-uploaded (i.e., provide for "stay-down"). If the content is not taken down, the rightsholder can apply to the Radio and Television Commission of Lithuania to issue a decision ordering ISPs to block their users' access to the site. The Commission has 14 days to issue the decision, which is subsequently approved by a Lithuanian court within a three-day window.*

Malaysia *[static and dynamic]. In Malaysia, website blocking exists on the basis of Section 263 of the Malaysian Communication and Multimedia Act 1998, which allows the Malaysian Communications and Multimedia Commission (MCMC) to issue orders requiring all registered ISPs to block access to copyright-infringing websites. In February 2020, Malaysia began blocking the IP addresses of servers found to be hosting pirated content.[204] Previously, only sites that provided illegal content through Android TV boxes were targeted.[205] A 2020 study*

---

200 Andy Maxwell, "Italian Soccer League Obtains Dynamic Pirate IPTV Blocking Order," Torrent Freak, September 28, 2021, https://torrentfreak.com/italian-soccer-league-obtains-dynamic-pirate-iptv-blocking-order-210928/ ; Andy Maxwell, "Court Orders ISPs to Block 56 'Pirate' IPTV Servers Over Serie A Piracy," Torrent Freak, June 19, 2020, https://torrentfreak.com/court-orders-isps-to-block-56-pirate-iptv-servers-over-serie-a-piracy-200619/.

201 Glyn Moody, "Bulk block of pirate streaming sites ordered by Italian court," ars technical, November 9, 2016, https://arstechnica.com/tech-policy/2016/11/bulk-block-pirate-streaming-sites-ordered-italian-court/.

202 [Translated] "Latvia's Electronic Mass Media Law," https://likumi.lv/ta/id/214039-elektronisko-plassazinas-lidzeklu-likums?version_date=01.01.2019#p-660434 ; Andy Maxwell, "New Law Will See Pirate TV Services Blocked By ISPs in Latvia," Torrent Freak, January 2, 2019, https://torrentfreak.com/new-law-will-see-pirate-tv-services-blocked-by-isps-in-latvia-190102/.

203 European Union Intellectual Property Office (EUIPO), Study on Dynamic Blocking Injunctions in the European Union (Brussels: EUIPO, March, 2021), https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Dynamic_Blocking_Injuctions/2021_Study_on_Dynamic_Blocking_Injuctions_in_the_European_Union_FullR_en.pdf.

204 Alexander Wong, "Malaysian authorities start blocking servers that stream pirated content, "Soyacincau, February 28, 2020, https://soyacincau.com/2020/02/28/malaysia-block-server-ip-illegal-copyright-streaming-android-tv/.

205 "Over 240 illegal streaming sites have been blocked by MCMC to curb content piracy," Soyacincau, February 4, 2019, https://soyacincau.com/2019/02/04/movie-streaming-sites-blocked-mcmc/.

finds that Malaysia's robust website-blocking practices have led to a 64 percent decrease in consumers accessing piracy websites. In 2019, fully 61 percent of Malaysian online consumers reported having visited piracy sites, but by 2020, that number had dropped to 22 percent.[206]

Netherlands *[static, dynamic, and live]. In 2020, The Amsterdam Court of Appeal (CoA) issued a dynamic blocking injunction against two Dutch ISPs aimed at blocking access to "mirror sites" of blatant piracy sites such as The Pirate Bay. The order cited the 2017 CJEU decision that sites such as The Pirate Bay may be blocked on IP-protection grounds.*[207] *Furthermore, Dutch courts have granted FAPL (the organizer of the Premier League competition of English professional soccer) a dynamic injunction to ask ISPs to block illegal streaming platforms before and during matches.*[208] *In 2021, Dutch rightsholders and ISPs created a landmark website-blocking agreement stating that if a court orders one ISP to block a site, the other ISPs will do the same.*[209] *This follows the CoA's final decision in regard to The Pirate Bay (as previously detailed). The Dutch government was involved in the development of the agreement, including the Authority for Consumers & Markets (ACM), to ensure that the plan would not violate net neutrality regulation (which it has stated it doesn't).*

Norway *[static]. In 2015, Norway first ordered local ISPs to block the top-level domains of multiple torrent file sharing sites notorious for piracy—specifically The Pirate Bay.*[210] *However, aside from the six sites blocked in this order, it does not appear that Norway has maintained a program of blocking piracy websites, either through established mechanisms or ad hoc requests.*

Peru *[static]. In 2020, Peru's Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intellectual (INDECOPI) issued blocking injunctions requiring ISPS to block access to Y2mate.com (the most popular stream-ripping site in the country) and streams associated with a local piracy-based set-top box provider (America TVGO).*[211]

Portugal *[static, dynamic, and live]. In 2015, Portugal set up a voluntary process in an agreement between ISPs, rightsholders, and the Ministry of Culture and the Association of Telecommunication Operators to block websites engaged in large-scale piracy.*[212] *The voluntary procedure involves the governmental body responsible for cultural affairs (IGAC) which reviews rightsholders' complaints, which can be filed in respect of "predominantly copyright infringing websites." Within 15 days after the filing of the complaint, IGAC can order ISPs to block access to the websites, and those blocks must remain in place for one year. In December 2018, the memorandum of understanding was amended to allow for the "live blocking" of sports.*

---

206 "Huge decrease in levels of streaming piracy seen in Malaysia over the last 12 months," press release, AVIA, September 17, 2020, https://avia.org/huge-decrease-in-levels-of-streaming-piracy-seen-in-malaysia-over-the-last-12-months/.

207 Eleonora Rosati, "CJEU says that site like The Pirate Bay makes acts of communication to the public," The IPKat, June 14, 2017, https://ipkitten.blogspot.com/2017/06/breaking-cjeu-says-that-site-like.html.

208 Court of the Hague, "case number / roll number: C/09/485400 / HA ZA 15-367," January 24,2018, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2018:615.

209 "Agreement between ISPs and copyright holders on blocking websites with illegal content after court ruling," press release, BREIN, November 5, 2021, https://stichtingbrein.nl/overeenstemming-tussen-internetaanbieders-en-auteursrechthebbenden-over-blokkeren-van-websites-met-illegale-content-na-uitspraak-van-de-rechter/.

210 Paul Resnikoff, "For the First Time In Norwegian History, Pirate Sites Are Being Blocked," Digital Music News, September 2, 2015, https://www.digitalmusicnews.com/2015/09/02/norwegian-court-orders-sweeping-blocks-against-the-pirate-bay-other-torrent-sites/.

211 International Intellectual Property Alliance (IIPA), "IIPA Written Submission in Response to USTR's Request for Comments and Notice of a Public Hearing Regarding the 2021 Special 301 Review" (IIPA submission, January 28, 2021), https://www.iipa.org/files/uploads/2021/01/2021SPEC301REPORT.pdf.

212 Andy Maxwell, "Rapid Pirate Site Blocking Mechanism Introduced By Portugal," Torrent Freak, July31, 2015, https://torrentfreak.com/rapid-pirate-site-blocking-mechanism-introduced-by-portugal-150731/.

Romania *[static]. In 2018, a Romanian court sided with rightsholders and agreed that ISPs should block (through DNS blocks) access to dozens of piracy sites.*[213]

Russia *[static and dynamic]. In 2017, Russian telecoms regulator Rozcomnadzor ordered local ISPs to block 8,000 pirate websites, a fourfold increase over 2016.*[214] *Russia allows that the blocking of piracy websites contributed to the growth of cinema box office revenues by 10.9 percent rightsholders to block pirate sites and any mirror sites. Rozcomnadzor claims that the blocking of piracy websites contributed to the growth of cinema box office revenues by 10.9 percent.*[215]

Saudi Arabia *[ad hoc]. Saudi Arabia first began website blocking by blocking access to The Pirate Bay in 2014. However, the country currently does not have an established legal framework for ordering injunctions against ISPs.*[216] *In 2020, Saudi authorities announced that the kingdom "continues" efforts to minimize Violations by blocking 231 sites that violated law.*[217]
Singapore *[static and dynamic].In 2014, important amendments to the Copyright Act were adopted, allowing rightsholders to obtain an injunction against access providers in respect to i infringing websites ("flagrantly infringing online locations").Following a2018 order to block 53 piracy sites comprising 154 unique web addresses, in 2020,an additional 17 sites and 41 domains were ordered blocked.*[218] *Singapore currently has the lowest rate of pirated content viewership in the Asia-Pacific (just 17 percent). In July 2018, the Singapore High Court confirmed the availability of dynamic site blocking orders.*

South Korea *[static]. South Korea is one of the most prolific sites blockers in the Asia-Pacific region.*[219] *Website blocking is available under an administrative procedure involving government authorities. As of early 2021, over 180 domains have been blocked, including popular BitTorrent sites and cyberlockers. In January2019, a new center was launched by the Korea Communications Standards Commission to deal with site-blocking applications more quickly as part of its overall mission to tackle piracy.*

Spain *[static, dynamic, and live]. In April 2021, a new blocking protocol was signed by rightsholders, ISPs, and the government to strengthen the protection of IP rights on the Internet, including the use of dynamic site blocking. The protocol was endorsed by Spain's Ministry of Culture. The protocol creates a new procedure for rightsholders to seek swift website blocks of new mirror domains whose exclusive or main purpose is to facilitate access to infringing websites that are already subject to site-blocking orders. Basically, it targets mirror or*

---

213 "Internet users in Romania won't be able to access websites with pirated movies," Romanian-Insider.com, November 7, 2018, https://www.romania-insider.com/internet-users-romania-ban-websites-pirated-movies.

214 [Translated] Daniil Kuzin, "Pirate websites are blocked four times more often," Izvestia, March 19,2018, https://iz.ru/716951/daniil-kuzin/piratskie-saity-stali-blokirovat-v-chetyre-raza-chashche.

215 Ibid.

216 Motion Picture Association – Canada, "Submission to the Canadian Radio-television and Telecommunications Commission on the proposal to disable access to piracy sites," Torrent Freak, March 29, 2018, https://torrentfreak.com/images/mpa-can.pdf.

217 Andy Maxwell, "Saudi Arabia Announces Launch of Pirate Site Blocking Campaign," Torrent Freak, June 22, 2020, https://torrentfreak.com/saudi-arabia-announces-launch-of-pirate-site-blocking-campaign-200622/.

218 Nigel Cory, "The Normalization of Website Blocking Around the World in the Fight Against Piracy Online," Innovation Files blog, June 12, 2018,https://itif.org/publications/2018/06/12/normalization-website-blocking-around-world-fight-against-piracy-online; "Singapore High Court blocks popular piracy streaming websites and illicit streaming device applications," press release, AVIA, July 6, 2020, https://avia.org/singapore-high-court-blocks-popular-piracy-streaming-websites-and-illicit-streaming-device-applications/.

219 Ernesto Van der Sar, "South Korea Expands Site Blocking Efforts with SNI Eavesdropping," TorrentFreak, February 14, 2019, https://torrentfreak.com/south-korea-expands-site-blocking-efforts-with-sni-eavesdropping-190214/.

subdomains whose purpose is to circumvent or avoid existing court-ordered blocking measures. The protocol creates a new entity, the Technical Committee, to implement and monitor the protocol. It includes representatives from ISPs and rightsholder groups. The protocol itself is subject to review. In2020, Spanish authorities ordered ISPs to dynamically block streams primarily of pirated soccer matches.[220] The order also named 44 pirate sites, requiring that their URLs, domain names, and IP addresses be blocked within 72 hours. As part of the dynamic blocking system, it allows broadcasters to notify ISPs of new sites, URLs, domains, and IP addresses every week for blocking without having to refer to the court for permission.

***Sweden** [static and dynamic]. Although previously refusing to block piracy sites such as The Pirates Bay, as of 2020, Swedish courts have approved an extendable, dynamic injunction against four major piracy sites.[221] This is the first instance of dynamic blocking in Sweden, and it allows rightsholders to expand the blocklist whenever these same piracy sites shift to new URLs.*

***Thailand** [static and dynamic]. In 2020, Thailand's Department of Intellectual Property (DIP), the Ministry of Digital Economy and Society (DES) and the National Broadcasting and Telecommunications Commission (NBTC) unveiled new website-blocking provisions for piracy sites that violate section20 (3) of the Computer Crimes Act (CCA). Under the new provisions, ISPs have 15 days to comply with the court orders and block sites, including proxy sites.[222]*

***United Kingdom** [static, dynamic, and live]. Since 2011, the United Kingdom has blocked hundreds of websites.[223] As with other European countries, protecting the copyright of Premier League matches is a priority for the United Kingdom, and the ability to issue dynamic and live blocking orders was renewed in 2018.[224] U.K. courts have also granted live and dynamic injunctions to Matchroom, which hosts live streams of professional boxing matches.[225] As detailed in this report, U.K. courts have also granted injunctions targeting piracy cyberlockers and stream-ripping sites.*

***Uruguay** [static]. In April 2018, Fox Networks Group Latin America obtained a website-blocking injunction in Uruguay against the website Redirect.[226]*

***Vietnam** [ad hoc]. In 2019, Vietnam's Authority of Broadcasting and Electronic Information (ABEI) ordered a telecommunications company to block access to the website xoilac.tv that was*

---

220 Santiago Millan Alonso, "A judge opens the way for the rapid blocking of pirate pay TV websites," El Pais Economia, February 18, 2020,https://cincodias.elpais.com/cincodias/2020/02/17/companias/1581968788_082002.html; Andy Maxwell, "Court Gives 'Dynamic' Pirate Site-Blocking the Green Light in Spain," Torrent Freak, February 20, 2020, https://torrentfreak.com/court-gives-dynamic-pirate-site-blocking-the-green-light-in-spain-200220/.

221 Samuel Gibbs, "Sweden refuses to order ISP to block Pirate Bay," The Guardian, November 30,2015, https://www.theguardian.com/technology/2015/nov/30/pirate-bay-stockholm-district-court-sweden-refuses-order-isp-block-site ; Ernesto Van der Sar, "Swedish Court Issues 'Dynamic' Pirate Bay Blocking Order," Torrent Freak, January 24, 2020, https://torrentfreak.com/swedish-court-issues-dynamic-pirate-bay-blocking-order-200124/.

222 Colin Mann, "Thailand: Anti-piracy website," Advanced Television, August 6, 2020, https://advanced-television.com/2020/08/06/thailand-anti-piracy-website/.

223 "Blocked Websites," TalkTalk website, https://community.talktalk.co.uk/t5/Articles/Blocked-websites/ta-p/2204638#11714.

224 Jeremy Dickerson, "Premier League "live" blocking order against livestream servers renewed for2017/18 season," Lexology, August 2, 2017, https://www.lexology.com/library/detail.aspx?g=a68db02f-12f5-4169-aa8f-56d35395d3b5.

225 "Matchroom Boxing Ltd & Anor v British Telecommunications Plc & Ors [2018]," England and Wales High Court, September 20, 2018, https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2018/2443.html&query=IL-2018-000155+.

226 Andy Maxwell, "Fox Networks Obtains Piracy Blocking Injunction Against Redirect," TorrentFreak, April 5, 2018, https://torrentfreak.com/fox-networks-obtains-piracy-blocking-injunction-against-rojadirecta-180405/.

transmitting sporting events without a license. However, Vietnam currently does not have an established legal framework for ordering injunctions against ISPs, so it appears that the blocking order was made based on Article 5(3) of the Joint Circular 07/2012 (on obligations of intermediary service providers in protection of copyright and related rights on the internet and telecom network environments). While this was a positive development, there is still significant uncertainty as to the scope of this provision and the availability of website blocking as a remedy, and a transparent documented process that sets out how to submit sites for blocking is needed.[227] "

[End of Annex 3 and of document]

[227] Duc Anh Tran and Loc Xuan Le, "Vietnam: Is site blocking the solution to online piracy?," Managing IP blog post, November 22, 2019, https://www.managingip.com/article/b1kbm1l4gl5zx5/vietnam-is-site-blocking-the-solution-to-online-piracy.