Harvard Journal of Law & Technology
Volume 38, Number 3 Symposium 2024

COMPARATIVE ONLINE BAD GUYS

*Justin Hughes**

ABSTRACT

Applying copyright to the internet required settling some initial, foundational questions: are digital copies reproductions?, is transmission of a copy through the internet an act of distribution?, etc. But once these were settled, copyright law on the internet has largely been shaped by the problem of efficient enforcement and what role internet intermediaries should play in that enforcement.

One of those on-going debates is about site-blocking, that is copyright owners obtaining court orders that require internet service providers to deny consumer access to pirate websites. Today, courts in dozens of jurisdictions — most of them representative democracies with robust civil rights — have promulgated such site-blocking or access denial orders. And an increasing number of those jurisdictions are making the injunctions "dynamic," that is, allowing the copyright owners to add new domain names, IP addresses, and URLs to the injunction with minimal court procedures.

Courts and legislators have grappled with the standards for blocking orders, particularly how to identify what the Delhi High Court calls "rogue sites" and what Singaporean law now calls "flagrantly infringing online location[s]." In these situations, courts and legislatures have been developing criteria that are expected to be used *iteratively* to sort culpable actors from more innocent participants in the digital network — *in litigations in which the alleged culpable actor is almost certainly not participating*.

Using developments in Australia, Singapore, India, and other jurisdictions, the Article explores whether there is an emerging consensus on how we identify the *bad guys*, at least when it comes to commercial scale copyright infringement on the internet.

---

* Honorable William Matthew Byrne, Jr. Professor of Law, Loyola Law School, Loyola Marymount University; Visiting Professor, Faculty of Law, Oxford University. My thanks to Richard Arnold, Rafael Jimenez Rosas, Daniel Jongsma, Daphne Keller, Howard Knopf, Loy Wee Loon, Nari Lee, Jack Lerner, Saw Cheng Lim, Miriam Marcowitz-Bitton, Alex Reinert, Thomas Riis, Arul George Scaria, George Spedicato, and Lauren Willis for helpful comments and suggestions on this project at various stages. Also, thanks to participants in the annual *ATRIP* conference, University of Tokyo (2023) and the *Role of Intellectual Property Remedies Symposium*, New York University (2024) for their suggestions and comments. Finally, thanks to research assistants Jillian Alexander, Timaj Kalifa, Andres Perez, and Fausto Polanco along with research librarian Laura Cadra. The remaining errors are the exclusive intellectual property of the Author.

TABLE OF CONTENTS

I. INTRODUCTION

In applying copyright law to the internet, the foundational questions were whether digital copies constituted reproductions under copyright law, whether network transmission of those copies triggered copyright's right of distribution, and whether streaming was public performance or making available as copyright understands those

concepts. All these questions were answered in the affirmative in court decisions, national legislation, and international treaties.[1]

But once all that was settled, copyright law on the internet has largely been shaped by the problem of *efficient enforcement.* For copyright owners to have effective enforcement in the digital, networked environment, copyright has had to deal repeatedly with the "elephants and mice" problem. In a 1998 article, Peter Swire succinctly described the enforcement challenge of the internet:

> In brief, elephants are large organizations that have major operations in a country. Elephants are powerful and have a thick skin but are impossible to hide. They are undoubtedly subject to a country's jurisdiction. Once legislation is enacted, they likely will have to comply. By contrast, mice are small and mobile actors, such as pornography sites or copyright violators, that can re-open immediately after being kicked off of a server or can move offshore. Mice breed annoyingly quickly — new sites can open at any time. Where harm over the Internet is caused by mice, hidden in crannies in the network, then traditional legal enforcement is more difficult. In such instances legal enforcement, to be successful, will focus on someone other than the mice themselves.[2]

In a prescient analysis, Swire identified internet service providers ("ISPs") as candidate "elephants" — targets for law enforcement on the internet.[3] When it comes to copyright law enforcement, commentators have agreed: regulation of ISPs and intermediary platforms —

---

1. Not necessarily in that order. The parties to the WIPO Copyright Treaty ("WCT") agreed that "[t]he reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder, fully apply in the digital environment, in particular to the use of works in digital form" and that "the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention." WIPO Copyright Treaty, Agreed Statement 1, Dec. 20, 1996, S. TREATY DOC. NO. 105-17 (1997), 2186 U.N.T.S. 121. The WCT also establishes a broad "right of communication to the public" that gives copyright holders the "exclusive right of authorizing any communication to the public of their works, by wire or wireless means." *Id.* at Article 8. In the United States, early court decisions determined that digital copies made and transmitted through the internet triggered the rights of reproduction and distribution. *See, e.g.*, Playboy Enters. v. Frena, 839 F. Supp. 1552, 1557 (M.D. Fla. 1993); Marobie-Fl v. Nat'l Ass'n Fire Equip. Distribs., 983 F. Supp. 1167, 1173 (N.D. Ill. 1997); Playboy Enters. v. Webbworld, Inc., 991 F. Supp. 543, 551 (N.D. Tex. 1997).

2. Peter Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991, 993 (1998) [hereinafter *Of Elephants*]; Peter Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, 153 U. PA. L. REV. 1977, 1999–2000 (2005).

3. *Of Elephants*, *supra* note 2, at 993.

imposing responsibilities, if not liabilities — is a substantially more cost-effective means of curbing copyright infringement in the networked environment than pursuing individual infringers.[4]

Not surprisingly, the development of internet copyright law has largely been a series of chapters on the relationship between copyright owners and "elephant"-sized intermediaries, whether ISPs, major (legitimate) platforms, or large pirate sites (of the kind that seek to become mainstream, if not legitimate). These chapters have been somewhat chronological, but also overlapping. This Article explores one of the more recent chapters: website-blocking in which content owners obtain court orders for ISPs to block internet users' access to "rogue" websites. Among all the stories of copyright owner/elephant relationships, site-blocking is also interesting because it is one in which the United States has played no role at all.

Part II sets the stage by briefly describing other chapters in copyright owners' relationship with the "elephants." These include the legislative decision in the early days of the internet to absolve neutral ISPs and internet platforms of responsibility to police the network for copyright infringement, while nonetheless giving platforms and services an obligation to disable or "take down" infringing websites when alerted by copyright owners. Subsequent chapters include the struggle to get ISPs to reveal information about alleged infringers; courts in various jurisdictions imposing liability on large, peer-to-peer ("P2P") system operators; and, after 2019, a raft of new laws in the European Union imposing new responsibilities on large online platforms.

The global development of judicially ordered website blocking ("site-blocking" or "access-denial") represents a distinct chapter of online copyright enforcement. In site-blocking, a court issues an injunction to specific ISPs ordering them to deny their customers access to specific locations on the internet that are known to be pirate websites. In the typical fact pattern, this occurs when the company or entity

4. *See, e.g.*, Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813, 818–19 (2001) ("[I]n the face of widespread private copying, copyright's traditional approach of direct legal action against each individual infringer would likely prove ineffective."); Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 655 (2003) (observing that careful ISP-level blocking regime could offer a "comprehensive scheme far more amenable to widespread content control both technically and as a matter of fairness to those censored"); Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 240 (2005) (exploring regimes for intermediary liability, including "'hot list' schemes in which the intermediary must avoid facilitation of transactions with certain parties"); David Lindsay, *Website Blocking Injunctions to Prevent Copyright Infringement: Proportionality and Effectiveness*, 40 U.N.S.W. L.J. 1507, 1507 (2017) ("[B]ringing actions against individual users is expensive, while regulating access via intermediaries is more cost-effective.").

running the pirate website is beyond the jurisdiction of the court, cannot be located, or simply refuses to participate in the litigation.

Part III describes the early development of site-blocking case law and the issues on which courts initially focused when granting site-blocking orders. Those issues have included court authority to grant such orders, the technical feasibility of site-blocking, the effectiveness of site-blocking, cost allocation between ISPs and copyright owners, and potential adverse impact on free expression. Part III also discusses how courts have made these injunctions increasingly "dynamic," allowing the prompt amendment or expansion of injunctions as pirate websites adopt new domain names, change IP addresses, and otherwise seek to evade law enforcement.

As of spring 2025 such site-blocking injunctions (normal and/or dynamic) have been issued by courts in over fifty jurisdictions on six continents.[5] In most of these cases, the courts have simply expressed satisfaction that the copyright owners have proven that the websites to be blocked are, in fact, "rogue websites," "pirate services," or "online locations that facilitate infringement of copyright." This kind of factual finding may be pretty straightforward when, for example, the service calls itself "The Pirate Bay."

But what to do when the rogue websites are not so clearly and stridently identifiable as infringement-based business models?[6] Part IV turns to this question, describing how multi-factor tests for when

---

5. World Intellectual Property Organization, Advisory Committee on Enforcement, *Study on the Effectiveness and the Legal and Technical Means of Implementing Website-Blocking Orders*, WIPO/ACE/17/13 (Dec. 31, 2024) https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_17/wipo_ace_17_13.pdf. Annex 3 of the study lists the following countries as "actively using website blocking" as of January 2022: Argentina, Australia, Austria, Belgium, Brazil, Canada, Colombia, Denmark, Ecuador, Finland, France, Germany, Greece, Iceland, India, Indonesia, Ireland, Israel, Italy, Latvia, Lithuania, Malaysia, the Netherlands, Norway, Peru, Portugal, Romania, the Russian Federation, Saudi Arabia, Singapore, South Korea, Spain, Sweden, Thailand, the United Kingdom, Uruguay, and Vietnam. This list is not complete; additional jurisdictions have upheld site-blocking. For Mexico, see *infra* note 101. For Kenya, see Ernesto van der Sar, *Pirate Site Blocking Expands to Kenya with Landmark Court Order*, TORRENTFREAK (June 28, 2022), https://torrentfreak.com/pirate-site-blocking-expands-to-kenya-with-landmark-court-order-220628/. *See also* Nigel Cory, *A Decade After SOPA/PIPA, It's Time to Revisit Website Blocking*, INFO. TECH. & INNOVATION FOUND. (Jan. 26, 2022), https://itif.org/publications/2022/01/26/decade-after-sopa-pipa-time-to-revisit-website-blocking/ [https://perma.cc/XNW7-RXS4]; Adam Mossoff, *Congress Should Protect the Rights of American Creators with Site-Blocking Legislation*, HERITAGE FOUND. (Feb. 14, 2024), https://heritage.org/crime-and-justice/report/congress-should-protect-the-rights-american-creators-site-blocking [https://perma.cc/S8KG-D52P] ("Some form of site blocking has been implemented in at least 40 countries.").

6. In the past, I have used "infringement-based business models" as a more neutral term. Justin Hughes, *On the Logic of Suing One's Customers and the Dilemma of Infringement-Based Business Models*, 22 CARDOZO ARTS & ENT. L.J. 725 (2005). Some courts have used similar phrases. *See, e.g.*, *Universal Music Australia Pty Ltd v TPG Internet Pty Ltd* [2017] FCA 435 (28 April 2017) ¶ 3 (Austl.) ("a business model that involves the distribution of infringing copyright material to Australian consumers").

websites will be subject to site-blocking orders have been established in Singapore, Australia, and India (the first two legislatively, the latter in a High Court decision). These are essentially frameworks for determining who the online bad guys are — especially when the bad guys cannot be brought to court.

The thesis of this Article is that such express, multi-factor tests for the identification of online bad actors — carefully calibrated and thoughtfully implemented by courts — can eliminate most of our free expression concerns from site-blocking as a mechanism for copyright enforcement. Part V proposes a set of criteria that should be useful for any decisionmaker seeking to ensure that the "bad guy" online locations — and only the bad guys — are blocked. While these criteria could be used by any sort of adjudicator — courts, administrative bodies, or self-policing private parties[7] — the focus here will be on court-ordered injunctions.

II. THE STORIED HISTORY OF COPYRIGHT OWNERS AND INTERNET ELEPHANTS

In the early years of widely-available internet access, governments settled on a compromise that an internet intermediary would not be liable for copyright infringements caused by its users as long as the intermediary acted promptly to disable access to the infringing material when so requested; the United States led this effort with the 1998 Digital Millennium Copyright Act ("DMCA")[8] followed by the European Union's 2000 E-Commerce Directive.[9] This formula — prompt disablement of infringing material when notified by copyright owners in exchange for a shield from financial liability[10] — became the

7. Blocking orders from administrative bodies has become the practice in Ecuador, Greece, Italy, Lithuania, and Spain. *See* Giancarlo Frosio & Oleksandr Bulayenko, *Website Blocking Injunctions in Flux: Static, Dynamic and Live*, 16 J. INTELL. PROP. L. & PRAC. 1127, 1130 (2021). For some discussion of private enforcement agreements, see *id.* at 1131.

8. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (relevant provisions codified in 17 U.S.C. § 512).

9. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular, Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) [hereinafter E-Commerce Directive]. The E-Commerce Directive does not expressly have "notice and takedown" provisions, but since the ISP must act "expeditiously" once it has knowledge of the alleged infringement, copyright owners can trigger such knowledge through notices. Some EU jurisdictions developed specific notice and takedown provisions. In France, Articles 6.I.2- 6.I.5 of the Loi pour la Confiance dans l'Economie Numérique ("LCEN") provided for a notice and takedown system. Loi 2004-575 du 21 juin 2004 loi pour la Confiance dans l'Economie Numérique [Law 2004-575 of June, 21 2004 Law on Confidence in the Digital Economy], JOURNAL OFFICIEL DE LA REPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], June 21, 2004. art. 6.I.2–.5.

10. At the time, this was understood to apply to hosting platforms and content storage services, not transmission ISPs. *See* 17 U.S.C. § 512(c), E-Commerce Directive, *supra* note 9, at art. 14.

centerpiece of internet copyright enforcement in the earliest days of the 21st century.[11]

One of the interesting aspects of this period is how this general consensus on the responsibilities of neutral internet providers within the copyright enforcement system appeared informally and almost organically, although it was later galvanized by bilateral and plurilateral treaties.[12] That "chapter" continues, and what was initially conceptualized as a human-operated notice system has now become largely automated across much of the internet with at least one piece of the U.S. domestic law — the § 512(d) provision for notice and takedown by search engines — becoming a *de facto* global enforcement mechanism.[13]

Meanwhile, there has been a distinct, on-going struggle between copyright owners and internet intermediaries both in Europe and the United States over whether and under what conditions intermediaries (ISPs and platforms) have to reveal the identity of users that the copyright owners were alleging to be infringers.[14] Those two narratives started in the early days of the internet and continue today.

Separately, at the beginning of the new millennium copyright owners dealt with a type of unforeseen intermediary: P2P platforms that were *intended* to provide unauthorized distribution of copyrighted works and did so on a massive scale that the copyright ecosystem had never seen before. Some of these platforms tried to operate as legitimate

---

11. Cheryl Foong & Joanne Gray, *From Little Things Big Things Grow: Australia's Evolving Site Blocking Regime*, 48 AUSTRALIAN BUS. L. REV. 352, 352–53 (2020) ("Intermediary safe harbours provided the key model for limiting the remedies flowing from copyright liability and enforcement responsibilities of online service providers, and the safe harbour model was propagated throughout the world . . . ."). For a near contemporaneous description of some of this, see Justin Hughes, *The Internet and the Persistence of Law*, 44 B.C. L. REV. 359 (2003).

12. A*ustralia-US Free Trade Agreement, Austl.-U.S.* art. 17.11, AUSTRALIAN GOV'T: DEP'T FOREIGN AFFS. & TRADE (May 18, 2004), https://www.dfat.gov.au/about-us/publications/trade-investment/australia-united-states-free-trade-agreement/Pages/chapter-seventeen-intellectual-property-rights [https://perma.cc/9TYH-LXEM] (limiting liability for service providers); *Dominican Republic-Central America FTA*, art. 15.11, WORLD BANK (Aug. 5, 2004), https://wits.worldbank.org/GPTAD/PDF/archive/UnitedStates-DominicanRepublic (CAFTA).pdf [https://perma.cc/4ACP-JS8R] (limiting liability for service providers).

13. *See Copyright Law in Foreign Jurisdictions: How Are Other Countries Handling Digital Piracy Before the S. Comm. on the Judiciary*, 116th Cong. 3 (2020) (statement of Professor Justin Hughes).

14. *See, e.g.*, Case C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH, ECLI:U:C:2009:107, ¶ 29 (Feb. 19, 2009) (holding that EU privacy laws do "not preclude Member States from imposing an obligation to disclose to private third parties personal data relating to Internet traffic to enable them to initiate civil proceedings for copyright infringements"); Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 262 (S.D.N.Y. 2008); EMI Records Ltd. v. Eircom Ltd. [2005] IEHC 233 (H. Ct.) (Ir.) (ordering ISP to disclose identities of allegedly infringer subscribers); BMG Canada Inc. v. John Doe, [2004] F.C. 488 (Can.); RIAA, Inc. v. Verizon, 351 F.3d 1229, 1231 (D.C. Cir. 2003); Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578–80 (N.D. Cal. 1999).

or quasi-legitimate businesses, but courts in multiple jurisdictions found them liable on the basis of similar, but differing, secondary liability regimes.[15]

In 2019, another distinct chapter in the legal relationship between copyright owners and *some* intermediaries began with the EU's Digital Single Market ("DSM") Directive.[16] Article 17 of the directive establishes a distinct regime of responsibility and liability for a sub-category of platforms called "online content-sharing service providers" ("OCSSPs").[17] While there are many exclusions from this category,[18] OCSSPs include Dailymotion, Facebook, Instagram, Vimeo, and YouTube.[19] Article 17 takes these OCSSPs out of the safe harbor provided by the EU's 2000 Electronic Commerce Directive[20] and requires them to obtain authorizations from copyright holders for public performances of works.[21] Otherwise, an OCSSP will be liable for infringement unless it has made "best efforts to ensure the unavailability" of any unlicensed copyrighted works.[22] This is widely understood to impose a filtering requirement on these platforms.[23]

---

15. *See, e.g.*, *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* [2005] FCA 1242 (5 September 2005) ¶ 520–22 (Austl.); Tōkyō Chihō Saibansho [Tokyo Dist. Ct.] Jan. 29, 2003, Heisei 14 (wa) no. 4249; The Winny Case [Kyoto District Court] Nov. 30 2004, Heisei 15 (wa); (US) A&M Records v. Napster, Inc., 239 F.3d 1004, 1027 (9th Cir. 2001); *In re* Aimster Litig., 334 F.3d 643, 656 (7th Cir. 2003); MGM v. Grokster, 545 U.S. 913, 940 (2005).

16. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, 2019 O.J. (L 130) [hereinafter DSM Directive].

17. *Id.* at art. 2(6) (defining OCSSP as "a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes").

18. DSM Directive at Article 2(6) excludes "not-for-profit online encyclopedias, not-for-profit educational and scientific repositories, open source software-developing and-sharing platforms" and business-to-business cloud platforms, while Article 17(6) excludes start-ups of a certain size. *Id.* at art. 2(6), 17(6).

19. As one law firm blog notes, "In most cases, it should be self-evident whether or not storing and providing public access to large amounts of uploaded content is a main purpose or merely incidental to another main purpose." Toby Headdon, *Am I an 'Online Content Sharing Service Provider' Under Article 17 (formerly Article 13) of the Proposed Copyright Directive*, BRISTOWS (Apr. 10, 2019), https://www.bristows.com/news/am-i-an-online-content-sharing-service-provider-under-article-17-formerly-article-13-of-the-proposed-copyright-directive/ [https://perma.cc/XHV3-SKXN].

20. DSM Directive, *supra* note 16, at art. 17(3). All other platforms remain in the E-Commerce Directive's regime. *See* Pamela Samuelson, *Pushing Back on Stricter Copyright ISP Liability Rules*, 27 MICH. TECH. L. REV. 299, 313 (2021).

21. DSM Directive, *supra* note 16, at art. 17(1).

22. DSM Directive, *supra* note 16, at art. 17(4).

23. *See, e.g.*, Marc Rees, *Directive Droit D'auteur: Déjà Une Mission Hadopi-CNC-CSPLA sur la Reconnaissance des Contenus*, NEXTINPACT (Mar. 28, 2019), https://www.nextinpact.com/news/107746-directive-droit-dauteur-deja-mission-hadopi-cnc-cspla-sur-reconnaissance-contenus.htm [https://perma.cc/QY4K-MYKT] (describing Article 17 as a notice and stay down system).

While this is a serious departure from the consensus international legal regime of 1998 onwards, for all practical purposes this copyright owner/intermediary narrative began at least as early as 2007, when YouTube first launched its "ContentID" system and made it clear that large platforms could offer operationally viable "takedown and *stay down*" services to copyright owners. We can speculate that YouTube's then new owner (Google) had a clear business reason for "ContentID": Google would make more money with YouTube if it could serve up at least *contextual advertising* and contextual advertising would require *knowing what the user is watching*.[24] It would have been a little difficult for Google to argue that, yes, they knew that the YouTube viewer was watching "South Park" for purposes of targeted advertising, but they did not know that the viewer was watching "South Park" for purposes of copyright infringement. And once YouTube "knew," the DMCA § 512 safe harbor would already be lost.[25]

III. THE LEGAL FRAMEWORK FOR SITE-BLOCKING

While the roles and responsibilities of neutral online platforms in copyright enforcement continue to evolve, a different combination of legislative and judicial activity is changing the responsibilities of transmission ISPs. Specifically, copyright owners have sought a more active enforcement role for these ISPs through court injunctions that require the ISPs to block access to websites dedicated to unauthorized distribution and streaming of films and music. Unlike early P2P systems, these "flagrantly infringing online locations" or "pirate websites"[26] are generally unlocatable and unresponsive to lawsuits.

As of 2025, such site-blocking orders have been issued by courts or administrative agencies in over 50 jurisdictions,[27] mainly in democratic societies with robust freedom of expression, including — but not limited to — the Danish Supreme Court,[28] the Italian Corte

---

24. Ana Gotter, *Contextual Advertising: What It Is and Why It Matters*, DISRUPTIVE (Jan. 15, 2018), https://disruptiveadvertising.com/blog/ppc/contextual-advertising [https://perma.cc/5963-4PFK]. For further discussion of targeted and contextual advertising, see Margot Kaminski, Jacob Snow, Felix Wu & Justin Hughes, *Symposium: The California Consumer Privacy Act*, 54 LOY. L.A. L. REV. 157, 184–87 (2020).

25. 17 U.S.C. § 512(c)(1)(A) (granting safe harbor unless platform has "actual knowledge" of infringement or is "aware of facts or circumstances from which infringing activity is apparent").

26. Different statutes, courts, and commentators use similar, but slightly different terms. For other terms, see Lindsay, *supra* note 4, at 1528 ("websites . . . for 'industrial scale' infringement").

27. *See supra* note 5.

28. U.2010.2221H (*Telenor v. IFPI*), Judgment of the Danish Supreme Court, 27 May 2010 (confirming an injunctive order against the service provider Telenor requiring Telenor to disable access to www.thepiratebay.org); *see also* U.2006.1474H, Judgment of the Danish

Suprema di Cassazione,[29] the Helsinki Court of Appeals,[30] the French Cour de Cassation,[31] the New Delhi and Madras High Courts,[32] the

Supreme Court, 10 Feb. 2006 (confirming that the service provider TDC's exemption from liability under Danish implementation of the E-Commerce Directive did not exempt TDC from an injunction to disable access to websites with illegal information); U.2015.1049.S, Judgment of the Danish Maritime and Commercial Court (Case A-38-14), 11 December 2014 (ordering ISP Telia Denmark to block access to UK-based online store based on copyright infringement).

29. Cass., 29 settembre 2009, n. 49437 (vacating decision by the Court of Bergamo and reinstating initial decision of the Court for Preliminary Investigations of Bergamo); *see also Italian Courts Affirm the Ban on The Pirate Bay*, IRIS MERLIN (2010), https://merlin.obs.coe.int/article/5269 [https://perma.cc/L3P8-QSM8]. For lower court decisions discussing further site blocking orders, see Trib. Milano, sez. spec., 8 maggio 2017; Trib. Milano, sez. spec. 12 aprile 2018; Trib Milano, sez. spec., 11 marzo 2019; Trib. Milano, sez. spec. 24 dicembre 2019; *see also* Trib. Milano, sez. spec., 22 maggio 2019 (extending the blocking order to domain name servers.

30. Finnish Nat'l Group of IFPI v. Elisa Oyj, No. 11/41552 (Helsinki District Court Oct. 26, 2011) (Fin.). On the basis of Section 60(c) of the Finnish Copyright Act, the court ordered one of Finland's biggest telecommunication providers, Elisa, to prevent access to Pirate Bay webpages. The decision was affirmed by the Helsinki Court of Appeals, decision number 1687, S 11/3097, June 15, 2012 and the Finnish Supreme Court denied leave to further appeal. Subsequent decisions in Finland ordering other ISPs to block Pirate Bay websites include Helsinki District Court decisions H11/48307 and H11/51544, both on June 11, 2012.

31. Cour de cassation [Cass.] [supreme court for judicial matters] Paris, July 6, 2017, Bull. civ. I, Nos. 16-17.217, 16-18.298, 16-18.348, 16-18.595 (recognizing site-blocking orders against ISPs, but requiring content owners to bear costs); *see also* Tribunal de Grande Instance, 3rd Division, 1st Section [TGI] [ordinary court of original jurisdiction] Paris, Apr. 2, 2015, No. 14/08177 (interlocutory judgment ordering T411 website to be blocked by several ISPs on the grounds that T411 was virtually entirely dedicated to making available audio recordings without authorization); Tribunal de Grande Instance, 3rd Division [TGI] [ordinary court of original jurisdiction, urgent applications section] Paris, Dec. 4, 2014, No. 14/03236 (ordering ISPs to block access in France to websites of the Pirate Bay network).

32. PTI, *Delhi HC Restrains 30 Torrent Sites from Hosting Copyrighted Content, Orders ISPs to Block Them*, FIN. EXPRESS (Apr. 11, 2019), https://www.financialexpress.com/india-news/delhi-hc-restrains-30-torrent-sites-from-hosting-copyrighted-content-orders-isps-to-block-them/1545480/ [https://perma.cc/5XUQ-5GFF]; Bill Toulas, *ISPs in India Ordered to Block Pirate Bay, Torrentz2, YTS, and 1337x*, TECHNADU (Apr. 12, 2019), https://www.technadu.com/isps-india-ordered-block-pirate-bay-torrentz2-yts-1337x/64592/ [https://perma.cc/TY77-CK7T]. In fact, Indian courts have been ordering ISPs to block pirate websites to protect new releases of Indian films for many years. Javed Anwer, *830 More Websites Blocked in India, Many Torrent Links in List*, INDIA TODAY (Aug. 25, 2016), https://www.indiatoday.in/technology/news/story/830-more-websites-blocked-in-india-many-torrent-links-in-list-337177-2016-08-25 [https://perma.cc/9LUL-64U5] ("Blocking of hundreds of URLs at the behest of film producers is not new in India. It has become almost routine to for film producers to approach court before release of a film and take John Doe orders, leading to the blocking of the websites. Not only torrent sites have been blocked under such orders but also image hosts, file hosts and websites that share URLs."); Anupam Saxena, *ISP Wise List of Blocked Sites #IndiaBlocks*, MEDIANAMA (May 17, 2012), https://www.medianama.com/2012/05/223-isp-wise-list-of-blocked-sites-indiablocks/ [https://perma.cc/H22J-R2PZ].

U.K. Supreme Court,[33] the Federal Court of Australia,[34] the Federal Court of Appeals in Canada,[35] the Federal Civil and Commercial Court in Argentina,[36] and the High Court of Singapore.[37]

Reviewing this case law across jurisdictions, especially the early decisions, it is clear that courts grappled with a common set of issues that touched on concerns shared by commentators.[38]

A. The Power of Courts or Administrative Authorities to Order Site-Blocking

The threshold issue is a court's power to issue site-blocking injunctions. Such power can arise either from an express legislative grant or from the inherent powers of the court, particularly a court with equitable powers in a common law jurisdiction.

1. Express Legislative Grants of Injunctive Power

Apart from the strange case of the United States (discussed below), the first law to provide for site-blocking injunctions to address copyright infringement was Article 8(3) of the European Union's 2001 Information Society Directive ("InfoSoc Directive"). Article 8(3) provides that "Member States shall ensure that rightholders 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."[39] The Court of Justice of the European Union ("CJEU") has

33. Cartier Int'l AG v. British Telecomms. PLC [2018] UKSC 28 (Trinity Term) (13 June 2018) [hereinafter *Cartier International*]. The High Court of Justice of England and Wales started issuing access denial injunctions in 2011. Twentieth Century Fox Film Corp. v. Brit. Telecomms. [2011] EWHC 1981 (Ch) [hereinafter *Newzbin2*]. The UK courts have continued to issue such injunctions, now with over a dozen decisions blocking hundreds on pirate sites. Richard Arnold, Website-Blocking Injunctions and Streaming Server-Blocking Injunctions: The State of the Art, Slide 7 (Dec. 3, 2020) (on file with the author).

34. *Roadshow Films Pty Ltd v Telstra Corp Ltd* [2016] FCA 1503 [hereinafter *Roadshow I*].

35. Bell Media Inc. v. GoldTV.Biz, [2019] FC 1432, *aff'd* TekSavvy Solutions Inc. v. Bell Media Inc., [2021] 4 F.C.R. 112 [hereinafter *TekSavvy*].

36. Juzgado Civil y Comercial Federal [Juzg. Fed. Civ. y Com.] (lower federal court in civil and commercial matters) 12/2022, "DirectTV Argentina SA c. Quien Resulte Responsibles (Does)," No. 10595/2022 [hereinafter *DirectTV Argentina*].

37. Disney Enterprises v. M1 Limited, [2018] SGHC 206 (19 September 2018) [hereinafter *Disney Enterprises*].

38. *See, e.g.*, Irene Calboli, *Legal Perspectives on the Streaming Industry: The United States*, 70 AM. J. COMPAR. L. i220, i242 (2022) ("[C]ourts should consider whether the injunction would significantly burden the provider's system or network, the extension of the harm to the copyright owner, the technical feasibility, effectiveness, and proportionality of the injunction.").

39. Article 8, Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the

consistently interpreted this language to provide for site-blocking injunctions.[40]

When the United Kingdom was part of the European Union, Article 8(3) of the InfoSoc Directive was implemented by Article 97A of the Copyright, Designs and Patent Act ("CDPA"), which was added in 2003 to give UK courts the "power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright."[41] The statute provides that actual knowledge is achieved by a notice from the copyright holder with "details of the infringement in question."[42] In its 2012 *Twentieth Century Fox v. British Telecommunications* decision, the High Court of England and Wales interpreted this liberally,[43] setting the stage for English jurists to be among the leaders in site-blocking decisions.[44]

Outside the European Union and United Kingdom, other jurisdictions have codified injunctive power for site-blocking. In Singapore, section 325 of the 2021 Copyright Act empowers the High Court to grant a site-blocking order directed at a network connection provider ("NCP") when an "online location is a flagrantly infringing online location" and "the NCP's services have been or are being used to access the online location."[45] Section 325 provides factors the court

---

Information Society, art. 8, 2001 O.J. (L 167) 10, 18 [hereinafter InfoSoc Directive]. This was reinforced by Article 11 of the EU's 2004 Enforcement Directive, which provides that "Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC." Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, art. 11, 2004 O.J. (L 195) 16, 23 [hereinafter Enforcement Directive].

40. L'Oréal S.A. v. eBay Int'l AG [2011] EWHC 1094 (Ch); Case C-494/15, Tommy Hilfiger Licensing LLC v. Delta Ctr., ECLI:EU:C:2016:528, ¶ 2 (July 7, 2016) ("[I]t [is] settled case-law that [these provisions oblige] member states to ensure that an intermediary whose services [are] used by a third party in order to infringe an intellectual property right could, regardless of any liability of its own, be ordered to take measures aimed at bringing those infringements to an end and measures seeking to prevent further infringements.").

41. Section 97A was added by The Copyright and Related Rights Regulations 2003, SI 2003/2498, art. 27, (Eng.). Jurisdiction for these injunctions is conferred on the High Court in England and Wales as well as the Court of Sessions in Scotland.

42. *Id.*

43. Justice Arnold reasoned that "the requirement for actual knowledge should not be interpreted too restrictively," Twentieth Century Fox Film Corp. v. Brit. Telecomms. [2011] EWHC 1981 (Ch) [146], and that the plaintiff need only show "that the service provider has actual knowledge of one or more persons using its service to infringe copyright." *Id.* at [148]. Section 191JA of the CDPA provides a parallel injunctive power to curb infringement of "a performer's property right." Copyright, Designs and Patent Act 1988, c. 48, § 191JA.

44. *Cartier International*, *supra* note 33, at ¶ 4 ("Since [two decisions in 2012] similar injunctions have been granted on 17 occasions against the appellant ISPs on the application of copyright-owners, and they have achieved a high degree of standardisation.").

45. Singapore Copyright Act of 2021, Section 325, https://www.wipo.int/wipolex/en/text/587174 [https://perma.cc/VB4K-7E6Y]. This provision was originally numbered section 193DDA(1) in the *Copyright Amendment Act 2014* (Singapore).

must consider in deciding whether or not to grant such an injunction, including several factors discussed below.

Similarly, Australian copyright law provides that a court may grant an injunction requiring an ISP "to take such steps as the Court considers reasonable to disable access to an online location outside Australia that . . . has the primary purpose or the primary effect of infringing, or facilitating an infringement, of copyright."[46] The Australian parliament's decision to limit the injunctive power to block "online location[s] outside Australia" is understandably rooted in the idea that the copyright holder in Australia may have no other practical relief against a foreign website, but it could have caused potential evidentiary problems.[47]

2. Inherent Powers of the Court

But a court's ability to issue site-blocking injunctions need not depend on specific copyright legislation, especially in a common law jurisdiction. In 2021, the Canadian Federal Court of Appeals concluded that such power exists under section 44 of Canada's Federal Court Act providing that courts may issue injunctions "in all cases in which it appears to the court to be just or convenient to do so"[48] and that this was particularly appropriate as injunctions are expressly seen as a form of relief available to copyright holders.[49] Although the United Kingdom codified injunctive relief in response to the Article 8(3) of the InfoSoc Directive, the legislative history shows an initial belief that U.K. courts could already issue such relief under the common law.[50] Indeed, in

46. *Copyright Act 1968* (Cth) s 115A(1) [hereinafter Australia Copyright Act].

47. As when a pirate website is headquartered abroad but uses proxy servers in Australia. Would the proxy servers suddenly make the pirate website located in Australia? Lindsay, *supra* note 4, at 1528. On the other hand, according to some commentators, practice has established a "rebuttable presumption that an online location is outside Australia, since it can be difficult to establish the location of a website and its owner." Michael Fraser & Henry Fraser, *Chapter 3: Australia*, *in* 1 COPYRIGHT THROUGHOUT THE WORLD § 3:42(a)(7) (Silke von Lewinski ed., 2024).

48. *TekSavvy*, *supra* note 35, at ¶ 19. The court specified that "the ISPs to whom [the injunction] applies are not defendants . . . and are not accused of any wrongdoing." *Id.* at ¶ 1.

49. *Id.* at ¶ 20 (citing section 34(1) of the Copyright Act, which entitles a copyright owner to "all remedies by way of injunction, damages, accounts, delivery up and otherwise that are or may be conferred by law for infringement of a right"). The court also noted that the Canadian Supreme Court had already ruled that "[t]he powers of courts with equitable jurisdiction to grant injunctions are, subject to any relevant statutory restrictions, unlimited." *Id.* at ¶ 19 (citing Google Inc. v. Equustek Sols. Inc., 2017 SCC 34, [2017] 1 S.C.R. 824, at ¶ 23).

50. At first, however, the Government stated that: "Regarding Article 8.3, it is already possible under UK law to seek injunctions against intermediaries." Richard Arnold, *Website-Blocking Injunctions: The Question of Legislative Basis*, 37 EUR. INTELL. PROP. REV. 623, 624 (2015). After consultations with rightholders concerned about uncertainty, the UK Government decided to legislate implementation of Article 8(3). *Id.* In contrast, in EMI

2018 the U.K. Supreme Court confirmed that British courts have the power to issue site-blocking injunctions to prevent trademark infringement (and, by implication, any other IP right) because "[f]or much longer than there has been an internet or EU Directives about it, the English courts have had jurisdiction in certain circumstances to order parties to assist those whose rights have been invaded by a wrongdoer."[51]

Germany is another jurisdiction where courts developed a site-blocking jurisprudence without specific statutory authorization; in fact, there was a conscious decision to *not* legislate domestic law enacting Article 8(3) of the 2000 InfoSoc Directive and to allow German courts to implement Article 8(3) via the application of *Störerhaftung*, a secondary liability doctrine in German law.[52] Germany has since codified *Störerhaftung* in relation to intellectual property claims, but at least the early site-blocking case law was based on the general power of the courts under the country's civil code. The Netherlands also initially chose not to codify judicial power to fulfill Article 8(3) of the 2001 InfoSoc Directive and only implemented specific language to address injunctions against third parties a few years later when Article 11 of the 2004 IP Enforcement Directive required Member States to provide courts with such power for *all IP rights*.[53]

Records [Ireland] Ltd. v. UPC Communications Ireland Ltd. [2010] IEHC 377, at ¶ 133, the Irish High Court concluded that it did not have power — under common law or the then-existing Irish copyright law — to issue a site-blocking injunction. Although Justice Charleton opined on such injunctive relief: "Were it available, I would grant it." *Id.* at ¶ 134.

51. *Cartier International, supra* note 33, at ¶ 8.

52. Arnold, *supra* note 50, at 629 ("[T]he [German] Government considered that the German doctrine of Störerhaftung (disturber liability or interferer liability) was sufficient to enable right holders to obtain injunctions against intermediaries."). *Störer* means interferer, in this case, an "interferer" with property rights. Under *Störerhaftung* a third party who played a role in the infringement can be liable unless it is unreasonable to burden the third party with a duty to examine whether his behavior could "interfere" with the (intellectual) property right at issue. The doctrine is based on BGB, § 1004. Frosio & Bulayenko, *supra* note 7, at 1132 & n.48.

53. Martin Husovec & Lisa van Dongen, *Website Blocking, Injunctions, and Beyond: View on the Harmonization from the Netherlands*, 12 J. INTELL. PROP. L. & PRAC. 695, 698 (2017):

> Finally, the Dutch law implemented an explicit legal basis in the separate IP acts for injunctions against intermediaries by amendment of March 2007. The third sentence of Art. 11 of the Enforcement Directive was implemented into all separate acts on IP rights, such as Art. 2(5) of the Database Act, Art. 17(2) of the Act on Original Topographies of Semiconductor products, Art. 70(2) of the Seeds and Planting Materials Act 2005 and . . . . Art. 26d of the Dutch Copyright Act and Art. 15e of the Neighbouring Rights Act. . . . While the articles across IP statues are adjusted for particular rights, the formulation used is essentially the same, namely that 'The court can at the request of the maker [order] ... intermediaries [,] whose services are being used by third parties to infringe copyright, [to suspend] those services used to make that infringement . . . .'.

3. The Mysterious Case of the United States

Federal courts in the United States have roughly the same range of equitable powers as courts in other common law jurisdictions, but absent specific federal legislation, Rule 65 of the Federal Rules of Civil Procedure might throw into question a federal district court's ability to order site-blocking as a preliminary injunction, the form of relief that copyright owners would most likely want. Rule 65(d)(2)[54] provides that preliminary injunctions bind only parties; the parties' officers, agents, servants, employees, and attorneys; and "other persons who are in active concert or participation" with any of these actors. ISPs are likely not in "active concert" with all the commercial and non-commercial websites that ISP users can reach.

But express, statutory injunctive relief was also part of the balanced package negotiated in the 1998 DMCA. While sections 512(a)–(d) shield intermediaries from monetary damages, section 512(j) makes ISPs expressly subject to different sorts of injunctive orders. For section 512(a) transmission ISPs, section 512(j)(1) provides the following:

> (B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms: . . . .
>
> (ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.[55]

The DMCA's legislative history provides little insight into this provision, basically repeating the language of the provision (as quickly or cautiously written legislative history in the United States often does). The legislative history expressly notes that "[s]uch blocking orders are not available . . . against infringing activity on a site within the United States or its territories."[56]

Many commentators have concluded that section 512(j)(1) empowers U.S. federal courts to issue site-blocking injunctions (at least

54. FED. R. CIV. P. 65(d)(2).

55. 17 U.S.C. § 512(j)(1)(B).

56. The Senate Judiciary Committee's report provides that "[t]he second form of relief, available in cases in which a provider is engaging in infringing activity relating to a foreign online location, is an order to take reasonable steps to block access to a specific, identified foreign online location. Such blocking orders are not available against a service provider qualifying under subsection (a) in the case of infringing activity on a site within the United States or its territories." S. REP. NO. 105-190, at 53 (1998); *see also* H.R. REP. NO. 105-551, at 62–63 (1998).

as to offshore pirate websites),[57] but the small number of cases litigating issues related to section 512 have not discussed injunctions against ISPs to block rogue websites.[58] While copyright owners express the view that section 512(j)(1) "provides an insufficient remedy for fighting copyright infringement both domestically and abroad,"[59] no stakeholder has clearly explained why the remedy is insufficient, at least not when most rogue websites are now believed to be hosted outside the United States.[60]

B. Feasibility, Effectiveness, Cost, and Proportionality

In the earlier site-blocking litigations, the technical feasibility of site-blocking was an issue commonly considered by courts.[61] Discussion of this issue generally subsided as it became *obvious* that site-blocking is technically feasible without, in the much-abused phrase, "breaking the internet."

Site-blocking can be achieved by preventing a domain name chosen by a user from reaching the matching IP address (domain name server ("DNS") blocking), blocking all access to a particular IP address (IP address blocking), Uniform Record Locator ("URL") blocking, blocking through deep-packet inspection, or some combination of these techniques. Courts and commentators have described the advantages

---

57. Calboli, *supra* note 38, at i242 ("In particular, the DMCA provides for three specific types of injunctions to use against service providers: identification of infringers, website blocking, and internet access suspension."); UNITED STATES COPYRIGHT OFFICE, REPORT ON SECTION 512 OF TITLE 17 169 n.907 (2020) (citing Professor Eric Goldman) [hereinafter USCO SECTION 512 REPORT].

58. USCO SECTION 512 REPORT, *supra* note 57, at 170. The USCO Report on Section 512 cites *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597 (9th Cir. 2018), as a case discussing section 512(j) injunctive relief, but the appellate decision does not actually cite section 512(j) and mentions only that the plaintiff initially sought injunctive relief. In fact, the plaintiff sought injunctive relief under California law, not section 512. Complaint at ¶ 49, 59, Ventura Content, Ltd. v. Motherless, Inc., No. 11-cv-05912, 2013 WL 12122569, (C.D. Cal. July 19, 2011). Regardless, since the litigation was between a copyright holder and a platform, it could not bear directly on the use of section 512(j) to seek an injunction against an ISP. Other cases are equally inapposite.

59. USCO SECTION 512 REPORT, *supra* note 57, at 169; *id.* at 193 ("Some rightsholders also advocated for a more extensive system of no-fault injunctions to address websites primarily dedicated to piracy."); *see also* Brooks Barnes, *Hollywood Sharpens Aim at Online Pirates*, N.Y. TIMES (June 24, 2024), https://www.nytimes.com/2024/06/24/business/hollywood-piracy.html [https://perma.cc/JQ8F-NRD3] (stating film studios have "started to campaign on Capitol Hill for a new tool: court-mandated site blocking").

60. Barnes, *supra* note 59 (reporting pirate sites for U.S. users moving offshore and, according to motion picture official, "The top three English-language piracy sites are all located in Vietnam."). In the understated view of the U.S. Copyright Office, "there may be some untapped 'potential' in section 512(j) for combating online infringement . . . ." USCO SECTION 512 REPORT, *supra* note 57, at 171.

61. Section 325(2)(c) Singapore Copyright Act of 2021 (requiring a court to consider "the technical feasibility of complying with the order"); *see also Disney Enterprises*, *supra* note 37, at ¶ 33 (satisfying the court that "DNS blocking, URL filtering or IP address blocking were technically feasible and did not place an excessive burden on the defendants").

and disadvantages of different approaches[62] and there is no need to replay that here.

Given those different methods, there is the question whether a court should specify the technical method to be used or should leave this to the ISPs. In its 2014 *UPC Telekabel Wien* decision,[63] the CJEU approved EU national courts using general "outcome prohibition" injunctions in which the court specifies *what* websites are to be blocked but leaves it to the defendant to decide *how*.[64] Most, if not all, courts — within and outside the EU — have done the same.[65] While this is probably preferable to both ISPs and copyright holders,[66] it has been criticized as leaving the question of "balance" between competing rights and interests in the hands of private parties.[67]

An analysis of the effectiveness of a potential site-blocking order may be required by statute[68] or simply be part of a court's proportionality analysis. As to effectiveness, empirical research on media consumption patterns in different countries has found "statistically and economically significant increases in usage of legal

62. *See, e.g.*, Twentieth Century Fox Film Corp. v. Brit. Telecomms. [2011] EWHC 1981 (Ch) [71] (describing technical means of site blocking); Maayan Perel, *Digital Remedies*, 35 BERKELEY TECH. L.J. 1, 23–27 (2020) (explaining different types of blocking); Nigel Cory, *How Website Blocking Is Curbing Digital Piracy Without "Breaking the Internet"*, INFO. TECH. & INNOVATION FOUND. (Aug. 2016), https://www2.itif.org/2016-website-blocking.pdf [https://perma.cc/AHR5-CZ8R]; Mossoff, *supra* note 5, at 16–17; Lindsay, *supra* note 4, at 1509–11.

63. Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, ECLI: EU:C:2014:192, (Mar. 27, 2014).

64. *Id.* at ¶ 66 (holding it is permissible "that injunction does not specify the measures which that access provider must take" and ISP "can avoid incurring coercive penalties for breach of that injunction by showing that it has taken all reasonable measures, provided that (i) the measures taken do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available and (ii) that those measures have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve").

65. *See, e.g.*, *Disney Enterprises*, *supra* note 37, at ¶ 33 (blocking methods "left largely within the discretion of the defendants").

66. Preferable because it preserves more freedom of action for the ISP, a point that the CJEU itself noted. Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, ECLI: EU:C:2014:192, ¶ 52 (Mar. 27, 2014).

67. Toumas Mylly, *Proportionality in the CJEU's Internet Copyright Case Law: Invasive or Resilient?*, *in* GENERAL PRINCIPLES OF EU LAW AND THE EU DIGITAL ORDER 267, 275 (Ulf Bernitz, Xavier Groussot, Jaan Pabu & Sybe A. de Vries eds., 2020) (arguing that this sort of injunction "allows delegation of decision-making power over fundamental rights from the judiciary to the private sphere"); Perel, *supra* note 62, at 39 ("[L]eaving service providers with broad discretion to elect how to implement a blocking injunction may result in encouraging them to apply the cheapest blocking techniques, regardless of their efficacy or accuracy."). I disagree with this speculation as ISPs must contend with the copyright owners (efficacy) as well as ISP users (accuracy).

68. Section 325(2)(d) Singapore Copyright Act of 2021 (requiring a court to consider "the effectiveness of the order").

media sites" following judicial site-blocking orders.[69] Generally speaking, courts have accepted that a site-blocking order need only reduce piracy coming from the blocked online locations and need not reduce infringement among all consumers.[70]

Site-blocking litigations have also dealt with the question of who should bear the costs of site-blocking, a question where the ISPs have a direct, bottom-line interest. According to Frosio and Bulayenko, the intermediaries bear the costs of implementing blocking injunctions in most European jurisdictions; this cost allocation is justified on different rationales, including that ISPs already internalize value from infringement occurring on their networks and so it is reasonable for them to contribute to the fight against online piracy.[71] In its 2016 *Roadshow Pictures* decisions, the Federal Court of Australia held that the ISP Telstra should pay the costs of setting up the technical arrangements to comply with Australia's statutory injunction regime,[72] while the copyright owners should pay the "compliance costs," i.e., the costs "of making the necessary entries in their DNS Blocking Systems to ensure that DNS blocking of the designated Domain Names is

69. Brett Danaher, Linon Sivan, Michael D. Smith & Rahul Telang, *The Impact of Online Piracy Website Blocking on Legal Media Consumption* (Mar. 12, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4723522 [https://perma.cc/B2PF-3U8N]; Brett Danaher, Jonathan Hersh, Michael D. Smith & Rahul Telang, *The Effect of Piracy Website Blocking on Consumer Behavior*, 44 MGMT. INFO. SYS. Q. 631, 633 (2020). Other studies, some sponsored by rightsholders, are not peer-reviewed and may be taken with a grain of salt. *See, e.g.*, RETTIGHEDSALLIANCE, ANNUAL REPORT 2018 7–8 (Feb. 2019), https://rettighedsalliancen.dk/wpcontent/uploads/2018/08/ENGB_RettighedsAlliancen2018.pdf [https://perma.cc/RE9M-VMUW] (average 75% decrease in Danish IP traffic to piracy sites following DNS blocking).

70. Christophe Geiger & Elena Izyumenko, *The Role of Human Rights in Copyright Enforcement Online: Elaborating a Legal Framework for Website Blocking,* 32 AM. U. INT'L L. REV. 43, 100–04 (2016).

71. Frosio & Bulayenko, *supra* note 7, at 1137–38 ("The intermediaries are bearing the costs of implementing a blocking injunction in most European jurisdictions. This is justified under the assumption that intermediaries (i) should contribute to the fight against online infringement, (ii) internalize value thanks to the infringement occurring on their networks, and (iii) are best positioned to end online infringements.").

72. *Roadshow I*, *supra* note 34, at ¶ 144 ("It seems to me that given the legislative environment in which the respondents have operated since the introduction of s 115A, it is not merely desirable but, practically speaking, essential that a CSP possess the technical capacity to comply with an injunction in the form agreed in these proceedings. Telstra's set-up costs are, in my opinion, a general 'cost of carrying on business' to borrow an expression used in the English authorities that have considered this question . . . . Moreover, they represent costs which I am satisfied Telstra would at some stage have had to incur irrespective of the existence of these proceedings.").

achieved."[73] In 2018, the U.K. Supreme Court reached a similar conclusion on cost-sharing between content owners and ISPs.[74]

Finally, courts in the European Union are obliged to ensure that site-blocking injunctions are "fair and proportionate," producing what is often called a proportionality analysis.[75] In the 2015 UK *Cartier* decision, Justice Arnold framed proportionality this way:

> [T]he key question on proportionality is whether the likely costs burden on the ISPs is justified by the likely efficacy of the blocking measures and the consequent benefit to [the rights holder] having regard to the alternative measures which are available to [the rights holder] and to the substitutability of the Target Websites.[76]

---

73. *Id.* at ¶ 145; *see also Foxtel Mgmt Pty Ltd v TPG Internet Pty Ltd* [2018] FCA 933, Order at ¶ 18 [hereinafter *Foxtel Management 2018* Order] (blocking order applicant to pay $AU 50 for each site blocked); *Foxtel Mgmt Pty Ltd v TPG Internet Pty Ltd* [2019] FCA 1450, Order at ¶ 18 [hereinafter *Foxtel Management 2019* Order] (blocking order applicant to pay $AU 50 for each site blocked).

74. *Cartier International*, *supra* note 33, at ¶ 5, 39 (declaring ISPs to bear:

> (i) the cost of acquiring and upgrading the hardware and software required to block the target sites [and] (ii) the cost of managing the blocking system, including customer service, and network and systems management" while content owners bear cost of "(iii) the marginal cost of the initial implementation of the order, which involves processing the application and configuring the ISP's blocking systems; (iv) the cost of updating the block over the lifetime of the orders in response to notifications from the rights-holders, . . . and (v) the costs and liabilities that may be incurred if blocking malfunctions through no fault of the ISP, for example as a result of over-blocking because of errors in notifications or malicious attacks provoked by the blocking.

75. Case C-324/09, L'Oréal SA, v. eBay Int'l AG, ECLI:EU:C:2011:474, [139] (July 12, 2011) (discussing measures set out in the Enforcement Directive "must be fair and proportionate and must not be excessively costly"); *id.* at ¶ 141 ("[I]njunctions which are both effective and proportionate may be issued against providers such as operators of online marketplaces.").

76. Cartier Int'l AG v. British Sky Broadcasting Ltd. [2014] EWHC 3354 (Ch) [261]. In *Cartier,* Justice Arnold listed seven considerations in judging the proportionality of a blocking injunction. Those factors were approved by the Court of Appeal and formulated as follows:

> (i) The comparative importance of the rights that were engaged and the justifications for interfering with those rights. (ii) The availability of alternative measures which were less onerous. (iii) The efficacy of the measures which the order require to be adopted by the ISPs, and in particular whether they will seriously discourage the ISPs' subscribers from accessing the Target Websites. (iv) The costs associated with those measures, and in particular the costs of implementing the measures. (v) The dissuasiveness of those measures. (vi) The impact of those measures on lawful users of the internet. In addition, it is relevant to consider the substitutability of other websites for the Target Websites.

Id. at [189]–[190]; *see also* Cartier Int'l AG v. British Sky Broadcasting Ltd. [2016] EWCA Civ 658 [127] (Kitchin, L.J.).

But as one commentator has observed, what courts call "proportionality" can be *either* a principle for balancing private party rights against other private party rights *or* a means/ends analysis that looks at whether the state's exercise of its power against private parties is reasonable and proportionate to the effects the state achieves.[77] Interestingly, "proportionality" in terms of the burden imposed on ISPs to protect the interests of copyright owners may be advanced *by the injunction allowing the ISP to choose the technical means of blocking* — precisely what some commentators think is an abdication of the court's role. There have been many criticisms of proportionality analysis[78] and, again, there is no need to recount all that here.

C. Dynamic Site Blocking

In many jurisdictions, site-blocking has become increasingly "dynamic," meaning procedures have been adopted to allow for the prompt addition of new domain names, IP addresses, and/or URLs to an existing site-blocking order[79] — and without filing a new lawsuit or appearing again before a court. Often courts grant dynamic or "adaptive" injunctions based on the general legislative grant to provide injunctive relief in this area.

Courts in the United Kingdom were among the first to grant dynamic site-blocking injunctions. In the 2011 *Twentieth Century Fox Film Corporation v. British Telecommunications* case, the injunction granted by the English High Court included a provision for the applicants to notify the respondent of additional IP addresses or URLs whose sole or predominant purpose was to enable or facilitate access to the *already blocked* Newzbin2 website.[80] After noting that Newzbin2 had already taken steps to evade blocking, Justice Arnold stated:

> I do not consider that [the applicants] should be obliged to return to court for an order in respect of

77. Lindsay, *supra* note 4, at 1512.

78. *See generally* Mylly, *supra* note 67, at 283–92; FRANCISCO J. URBINA, A CRITIQUE OF PROPORTIONALITY AND BALANCING (2017); Hugh Collins, *The Challenges Presented by Fundamental Rights to Private Law*, *in* PRIVATE LAW IN THE 21ST CENTURY (Kit Barker, Karen Fairweather & Ross Grantham eds., 2017).

79. Just a few of the courts that have embraced dynamic site-blocking include *Foxtel Management 2018* Order, *supra* note 73, at ¶ 13; *Foxtel Management 2019* Order, *supra* note 73, at ¶ 13; Rogers Media Inc. v. John Doe 1, [2022] FC 775 (Can.); *Bell Media, Inc. v. John Doe 2 dba Soap2day.to* Order, [2024] Docket: T-1125-23 (Can.). *See generally* EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE, STUDY ON DYNAMIC BLOCKING INJUNCTIONS IN THE EUROPEAN UNION (2021).

80. Twentieth Century Fox Film Corp. v. Brit. Telecomms. PLC [2011] EWHC 2714 (Ch) [12]. The litigation had two reported decisions. In Twentieth Century Fox Film Corp. v. Brit. Telecomms. PLC [2011] EWHC 1981 (Ch), Judge Arnold determined that a site-blocking injunction directed at the ISPs was appropriate; after subsequent briefing and agreement among the parties, the court opined on the scope of the injunction in the EWHC 2714 decision.

> every single IP address or URL that the operators of Newzbin2 may use. In my view the wording proposed by [the applicants] strikes the appropriate balance. If there is a dispute between the parties as to whether the predominant purpose of an IP address or URL is to enable or facilitate access to Newzbin2, they will be able to apply to the court for a resolution of the dispute.[81]

This has become a basic feature of site-blocking orders in the United Kingdom.[82]

In the European Union, the CJEU has interpreted provisions of EU law as giving courts the ability to issue orders that not only address the infringing activity before the court "but also [] prevent [] further infringements of that kind."[83]

Singapore's site blocking legislation similarly does not expressly discuss dynamic injunctions, but the Singapore High Court approved such an injunction in its 2018 *Disney Enterprises v. M1 Limited* decision.[84] Discussing how the infringing online locations had *already* changed some of their domain names and established mirror sites, the court found that a dynamic injunction met the statutory standard of "reasonable steps to disable access to the flagrantly infringing online location"[85] and that "[w]ithout a continuing obligation to block additional domain names, URLs and/or IP addresses upon being informed of such sites, it is unlikely that there would be effective disabling of access" to the online locations.[86]

The plaintiffs proposed that they would file affidavits with the defendant ISPs (filed contemporaneously with the court) identifying additional domain names to be blocked and providing reasons why the online locations accessible from the additional domain names are the

---

81. [2011] EWHC 2714 at ¶ 12.

82. *See* Cartier Int'l AG v. British Sky Broadcasting Ltd. [2016] EWCA Civ 658 [18] ("An important feature of all of the orders made pursuant to s 97A has been that they have included a provision for the rightholders to notify additional IP addresses or URLs to the ISPs in respect of the websites which have been ordered to be blocked. This has allowed the rightholders to respond to efforts made by website operators to circumvent the orders by changing their IP addresses or URLs.").

83. Case C-324/09, L'Oréal SA, v. eBay Int'l AG, ECLI:EU:C:2011:474, Ruling [7] (July 12, 2011). *L'Oréal* concerned whether an injunction could order an online platform to prevent further trademark infringements of the kind in suit, not a dynamic (changing) injunction per se. The Court was interpreting the third sentence of Article 11 of Directive 2004/48/EC (the enforcement directive) which has the same language providing for injunctive relief for all forms of intellectual property as Article 8(3) of the InfoSoc Directive provides for infringements of copyright and related rights.

84. [2018] SGHC 206.

85. *Id.* at ¶ 37–38.

86. *Id.* at ¶ 42.

same as the online locations subject to the initial injunction.[87] The court accepted this, but allowed that the ISPs need not comply where the ISP believed the "grounds for disabling access" to any additional domain names, URLs, or IP addresses was "insufficient."[88]

In Australia, the 2018 amendment of their site-blocking provisions allows for injunctions to "block domain names, URLs and IP addresses that the carriage service provider and the owner of the copyright agree, in writing, *have started to provide access to the online location after the injunction is made*."[89]

D. Addressing Free Expression Concerns

The potential impact of a site-blocking or access denial order on free expression should be a serious concern for everyone;[90] that concern is accentuated when a jurisdiction adopts a dynamic site-blocking regime that extends or alters a site-blocking order with only limited judicial review. Moreover, the adverse impact on free expression from site blocking is more intuitively concrete than amorphous concerns sometimes expressed about the adverse impact of site-blocking on "innovation."[91]

But the concern about free expression itself requires unpacking: there are the free expression interests of consumers, the free expression interests of the alleged pirate online locations, and any free expression interests of the ISPs.

The last of these should be rejected. To limit their liability, ISPs have consistently argued that they are not "speakers" in the sense of

87. *Id.* at ¶ 6. Similar procedures have been adopted in Denmark and the Netherlands. *See* Frosio & Bulanyenko, *supra* note 7, at 13–14.

88. [2018] SGHC 206, at ¶ 44.

89. *Copyright Act 1968* (Cth) s 115A(2B)(a)(ii) (emphasis added). There is a parallel provision to extend an injunction directed at a search engine to "not provide search results that include domain names, URLs and IP addresses that the online search engine provider and the owner of the copyright agree, in writing, have started to provide access to the online location after the injunction is made." *Id.* at 115A (2B)(b)(ii).

90. *See, e.g.*, Twentieth Century Fox Film Corp. v. Brit. Telecomms. [2011] EWHC 1981 (Ch) [199] (discussing copyright owners agreed that a site-blocking injunction "engaged the Article 10 [freedom of expression] ECHR rights of BT's subscribers"); USCO SECTION 512 REPORT, *supra* note 57, at 195 (citing free speech concerns with website blocking); Orit Fischman-Afori*, Online Rulers as Hybrid Bodies: The Case of Infringing Content Monitoring*, 23 U. PA. J. CONST. L. 351, 369 (2021) (stating a blocking order regime "raises concerns with respect to its impact on freedom of speech in the digital sphere"); Geiger & Izyumenko, *supra* note 70, at 52–76; Foong & Gray, *supra* note 11, at 353 ("[M]easures to safeguard the public interest in . . . access to information are not adequately built into the [Australian] regime"); Perel, *supra* note 62, at 28 (expressing view that all blocking methods have "robust collateral effects, which impact human rights").

91. *See* Mylly, *supra* note 67, at 277–78.

newspapers or broadcasters.[92] There may be more nuanced disagreement about whether search engine results or generative AI output is "speech,"[93] but when an entity is only providing a "network connection" they are not a speaker.[94] Whatever an ISP might try to present as their right to free expression really boils down to a right to conduct a business.[95]

In contrast, the free expression concern of consumers is widely, if not universally, recognized to include the right to receive information.[96] In Europe, this has been expressly recognized to include a "right to internet access,"[97] which nonetheless may be subject to varied restrictions.[98] But very few advocate that citizens of a democratic society have a "right" to access information whose distribution has been made illegal by long-standing laws of that same democratic society. This is true whether the prohibited distribution concerns

---

92. As Rebecca Tushnet has noted, "ISPs may be agents of free speech but that does not mean that they automatically take on the interests of every speaker whose speech they carry. By default, access providers . . . do not select or approve content and are not generally thought to do so. Just as a telephone company is not engaging in speech of its own when its users speak, ISPs generally facilitate others' speech rather than speaking for themselves." Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 1012 (2008).

93. *See* Eugene Volokh & Donald Falk, *First Amendment Protection for Search Engine Search Results*, 3 (UCLA School of Law, Research Paper No. 12-22, Apr. 20, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055364 [https://perma.cc/RC25-2WTL].

94. *See, e.g.*, *TekSavvy*, *supra* note 35, at ¶ 50 ("I have difficulty accepting that ISPs like Teksavvy engage in any expressive activity when they provide their customers with access to certain websites. As Teksavvy itself has argued, it acts as a common carrier subject to an obligation of net neutrality. . . . In this sense, its everyday activities in question are not expressive and therefore do not engage freedom of expression.").

95. In the European Union, the CJEU said that the freedom to conduct a business is implicated where an injunction constrains an ISP "in a manner which restricts the free use of the resources at his disposal because it obliges him to take measures which may represent a significant cost for him, have a considerable impact on the organisation of his activities or require difficult and complex technical solutions." Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, ECLI: EU:C:2014:192, ¶ 50 (Mar. 27, 2014).

96. On the European Union side, Article 10(1) of the EUROPEAN CONVENTION ON HUMAN RIGHTS provides that the right of free expression "include[s] freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." European Convention on Human Rights art. 10(1), Nov. 4, 1950, E.T.S. No. 5. Article 11(1) of the CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION uses the same language. Charter of Fundamental Rights of the European Union art. 11(1), Dec. 7, 2000 (2000 O.J. (C. 364). In the United States, the express right to receive information goes back at least to *Martin v. City of Struthers*, 319 U.S. 141, 143 (1943).

97. Ahmet Yıldırım v. Turkey, 3111/10 Eur. Ct. H.R. (2012) at ¶ 31 ("The right to Internet access is considered to be inherent in the right to access information and communication protected by national Constitutions and encompasses the right for each individual to participate in the information society and the obligation for States to guarantee access to the Internet for their citizens.").

98. *Id.* at ¶ 33 ("As regards possible restrictions in cases of illegal Internet content, European countries have adopted a wide variety of approaches and legislative measures, ranging from the suspension of individual rights of Internet access or the removal of the illegal content, to the blocking of access to the specific website in question.").

nuclear weapon designs, privacy violations, the trade secrets of others, or copyright works made available without authorization.

The free expression interests of internet users concern lawfully distributed information, at least in a society governed by laws that result from deliberative democratic processes and pass judicial muster.[99] In early 2025, administrative agency site-blocking in Italy appears to have caused episodes of overblocking;[100] there also appears to have been an incident of administratively-ordered overblocking in Mexico in 2017.[101] But to date, there is little or no empirical data to indicate that court-supervised access denial injunctions in *any jurisdiction* have caused internet users to be denied access to lawfully distributed news, information, entertainment, or discourse.[102]

Free expression concerns with court-supervised site-blocking are inextricably entwined with the question of proper identification of the "bad guys." Substantively, if we have the right filter to identify the

---

99. In the United States while courts have long recognized the right to receive information, Stanley v. Georgia, 394 U.S. 557, 564 (1969), this right does not extend to information whose distribution is illegal or unauthorized. Schnapper v. Foley, 667 F.2d 102, 112 (D.C. Cir. 1981) (stating the "doctrine that the First Amendment protects the right of the listener to receive information from a willing speaker" is irrelevant if access to copyrighted work was not authorized); Eldred v. Reno, 74 F.Supp.2d 1, 3 (D.D.C. 1999) ("[T]here are no First Amendment rights to use the copyrighted works of others."), *aff'd* 239 F.3d 372 (D.C. Cir. 2001), *aff'd* Eldred v. Ashcroft, 537 U.S. 186, 197 (2003); Dhiab v. Trump, 852 F.3d 1087, 1096 (D.C. Cir. 2017) ("[N]either the intervenors nor the public at large have a right under the First Amendment to receive properly classified national security information . . . ."); Woven Elecs. Corp. v. Advance Grp., Inc., 930 F.2d 913 (4th Cir. 1991) (unpublished table decision) (stating trade secrets are exception to public right to access information); Valley Broad. v. U.S. Dist. Ct., 798 F.2d 1289, 1294 (9th Cir. 1986) (same).

100. Letter from Computer & Communications Industry Association to Emmanuelle du Chalard, et al, European Commission (Jan. 21, 2025) (on file with author).

101. In 2017, the Second Chamber of the Mexican Supreme Court found that a site-blocking order issued by the Instituto Mexicano de la Propiedad Industrial was overbroad, but that site-blocking orders were permissible as against websites where the majority of copyrighted content is unauthorized. *See* Luis Schmidt, *"Most" Counts as "Total" when Blocking Websites in Mexico*, THE COPYRIGHT LAW. (Oct. 2017), https://www.olivares.mx/wp-content/uploads/2018/02/olivares-final-oct-17.pdf. The court noted that its ruling "does not prevent the responsible authority, in the exercise of its powers and in satisfying the constitutional and legal requirements for it, from issuing a new official letter in which it orders only the blocking of those specific contents that may be considered contrary to the copyright rights of third parties." (author's translation) Sentencia recaída al Amparo Directo en Revisión 1/2017. Alestra, S. de R.L. de C.V. Segunda Sala. 19 de abril de 2017, página 45. Ponente: Alberto Pérez Dayán. https://www2.scjn.gob.mx/ConsultasTematica/Detalle/209243 (Judgement to Amparo Appeal 1/2017. Alestra, S. de R.L. de C.V. Second Chamber. April 19, 2017. Reporting Judge: Alberto Pérez Dayán). Since that time, an appellate court in Mexico City has interpreted the Supreme Court's decision as permitting blocking of websites that are principally infringing content. Recurso de Queja Suspensión Provisional, Acuerdo del Vigésimo Tribunal Colegiado en Materia Administrativa del Primer Circuito [TC], 10 de abril de 2023, 158/2023. Moisés Castorena Katz, *The Blocking of Web Pages due to Stream Ripping in Mexico*, LEXOLOGY (Oct. 4, 2023), https://www.lexology.com/library/detail.aspx?g=8e888043-a995-451c-823f-80a0b3ea36b3.

102. Mossoff, *supra* note 5, at 20 (noting that "the overblocking criticism about court-ordered site blocking is almost entirely unsupported by the data").

flagrantly infringing online locations and *only* those online locations, collateral adverse impact on free expression should be minimal. Procedurally, both the alleged rogue website(s) and users should have means to challenge site blocks in court.[103] In the case of users, this necessarily includes replacing the blocked site with informational webpages explaining the court action so that a consumer understands why they are unable to access a particular online location, particularly because these pirate websites often mimic legitimate services and may have easily mistaken consumers.[104]

IV. FRAMEWORKS FOR IDENTIFYING ONLINE BAD GUYS

In site-blocking litigations courts make (and must make) some evidentiary determination that the online locations to be blocked are providing internet users with unauthorized access to copyright works. But most court opinions provide very little insight on the evidence before the court. For example, in its 2021 *TekSavvy Solutions* decision the Federal Court of Appeals of Canada did not opine on the standards for issuing a blocking order against an online location, noting only that it saw "no basis on which there could be any doubt that the defendants have and continue to infringe the plaintiffs' rights in copyright."[105] Other adjudicators make similar conclusory findings of fact[106] and such general statements do not provide any guidance going forward on this critical question.

But some legislatures and courts have put forward frameworks for identifying the "bad guys" who can and should be subject to website blocking. Let us consider developments in three jurisdictions.

---

103. *See, e.g.*, Football Association Premier League Ltd v. British Sky Broadcasting Ltd [2013] EWHC 2058 (Ch) [57–58] (applying an additional safeguard of expressly allowing operators of target websites to apply to vary or discharge a site-blocking order). The European Court of Human Rights has also required that site blocking regimes (other than copyright) include procedural safeguards for website owners and internet users. Engels v. Russia, 61919/16 Eur. Ct. H.R. (2020) at ¶ 32–34; Ahmet Yıldırım v. Turkey, 3111/10 Eur. Ct. H.R. (2012) at ¶ 68.

104. For some examples, see IP HOUSE, OVERSEAS AND OUT OF REACH: INTERNATIONAL VIDEO PIRACY AND U.S. OPTIONS TO COMBAT IT 9–11 (2024) (comparing visual appearance of Paramount+ to pirate sites 123movies.com and Flixvision.com).

105. *TekSavvy*, *supra* note 35, at ¶ 65.

106. *See, e.g.*, *DirectTV Argentina*, *supra* note 36 (concluding that the independent report "demonstrated that each of the denounced sites infringes or facilitates the infringement of copyrights, the illegal transmission of the signals and the content of the claimants" - *demostraría que cada uno de los sitios denunciados infringe o facilita la infracción a los derechos de autor, la transmisión ilegal de las señales y contenidos de las demandantes*); Finnish Nat'l Group of IFPI v. Elisa Oyj, No. 11/41552 (Helsinki District Court Oct. 26, 2011) (Fin.) (finding "the sharing of files distributed without the permission of the holders of the rights is the main reason why people use the The Pirate Bay service").

A. Singapore

The 2014 amendment of Singapore Copyright Law established what may have been the first express statutory framework for determining when a website was enough of a bad actor to be the subject of an access denial order.[107] Singapore law labels these websites "flagrantly infringing online locations" and provides that in "deciding whether an online location is a flagrantly infringing online location" the court should consider the following factors:

> (*a*) whether the primary purpose of the online location is to commit or facilitate rights infringement;
> (*b*) whether the online location makes available or contains directories indexes or categories of the means to commit or facilitate rights infringement;
> (*c*) whether the owner or operator of the online location demonstrates a general disregard for copyright or the protection of performances;
> (*d*) whether access to the online location has been disabled by orders from any court of another country or territory on the ground of or related to rights infringement;
> (*e*) whether the online location contains guides or instructions to circumvent measures, or any order of any court, that disables access to the online location on the ground of or related to rights infringement;
> (*f*) the volume of traffic at or frequency of access to the online location;
> (*g*) any other relevant matters.[108]

According to the statute, these factors are *not* optional: they "must be considered and the appropriate weight must be given to them."[109]

B. Australia

Australia followed Singapore in 2015, amending its copyright law to provide an express framework for the issuance of "[i]njunctions against carriage service providers providing access to online locations

---

107. Originally numbered 193DDA(2) in the *Copyright Amendment Act 2014* (Singapore), this provision was reassigned as Section 99 in the Singapore Copyright Act of 2021.

108. *Id.*

109. *Id.* As originally written in 2014, these factors said "copyright infringement" instead of "rights infringement"; "protection of performances" was missing from factor (c); and factor (g) was not there. So, the more recent amendment tweaked the factors to include protection of performances.

outside Australia."[110] (In Australia, ISPs are commonly called "carriage service providers.") After a subsequent amendment in 2018, Section 115A of their copyright law now provides:

> (1) The owner of a copyright may apply to the Federal Court of Australia to grant an injunction that requires a carriage service provider to take such steps as the Court considers reasonable to disable access to an online location outside Australia that:
>
> (a) infringes, or facilitates an infringement, of the copyright; and
>
> (b) has the primary purpose or the primary effect of infringing, or facilitating an infringement, of copyright (whether or not in Australia).

Originally, the language in section 115A(1)(b) said "the primary purpose of the online location is to infringe, or to facilitate the infringement of, copyright." That was changed to the "primary purpose or the primary effect" language in a 2018 amendment.[111] The 2018 amendment also added a provision expressly allowing the court to grant an injunction directed at a search engine to block search results leading to infringing online locations.[112]

Section115A(5) then sets out the factors which the court should take into account in determining whether to grant the injunction. Some of these factors address the interests of third parties and/or what we might call proportionality,[113] but several directly address determination that the sites to be blocked are, in fact, bad actors:

> (a) the flagrancy of the infringement, or the flagrancy of the facilitation of the infringement, as referred to in paragraph (1)(b);
>
> (b) whether the online location makes available or contains directories, indexes or categories of the means to infringe, or facilitate an infringement of, copyright;

---

110. *Copyright Act 1968* (Cth) s 115A.

111. *See* Foong & Gray, *supra* note 11, at 354 ("In 2018, the regime was expanded to also cover search engine providers and online locations that have the 'primary effect' (and not just primary purpose) of infringing or facilitating the infringement of copyright.").

112. *Copyright Act 1968* (Cth) s 115A(2) ("The application under subsection (1) may also request that the injunction require an online search engine provider (other than a provider that is covered by a declaration under subsection (8B)) to take such steps as the Court considers reasonable so as not to provide a search result that refers users to the online location.").

113. *See, e.g.*, *id.* at s 115A(5)(e) ("whether disabling access to the online location is a proportionate response in the circumstances"); *id.* at s 115A(5)(f) ("the impact on any person, or class of persons, likely to be affected by the grant of the injunction"); *id.* at s 115A(5)(g) ("whether it is in the public interest to disable access to the online location").

> (c) whether the owner or operator of the online location demonstrates a disregard for copyright generally;
> (d) whether access to the online location has been disabled by orders from any court of another country or territory on the ground of or related to copyright infringement . . . .[114]

A Section 115A injunction against an ISP can require it "to take reasonable steps to disable access" to the online location.[115] The legislative history of the initial 2015 amendment describes section 115A as "a key reform to reduce online copyright infringement"[116] and as ensuring that copyright owners could apply for injunctions for website blocking "without having to first establish the [ISP's] liability for copyright infringement or authorisation of copyright infringement."[117]

C. India

In the 2019 *UTV Software Communication Ltd v. 1337X.TO* litigation the Delhi High Court looked to these Singaporean and Australian laws in crafting a multi-factor analysis for determining whether an online location should be subject to a blocking order.[118] The court's factors will now be familiar:

> a. whether the primary purpose of the website is to commit or facilitate copyright infringement;
> b. the flagrancy of the infringement, or the flagrancy of the facilitation of the infringement;
> c. whether the detail of the registrant is masked and no personal or traceable detail is available either of the Registrant or of the user.
> d. whether there is silence or inaction by such website after receipt of take down notices pertaining to copyright infringement.

---

114. *Id.* at s 115A(5).

115. Parliament of Australia, House of Representatives, Explanatory Memorandum for Copyright Amendment (Online Infringement) Act of Bill, at ¶ 40, https://www.legislation.gov.au/bills/C2015B00052 [https://perma.cc/6XJZ-BTH7] [hereinafter House Explanatory Memorandum (Austl.)].

116. House Explanatory Memorandum (Austl.), at ¶ 1. The legislation was also described as "a precise response to a specific concern raised by copyright owners," and "a standalone injunction power which operates as a no-fault remedy." *Id.* at ¶ 7.

117. House Explanatory Memorandum (Austl.), at ¶ 3.

118. UTV Software Comm'n Ltd v. 1337X.TO, No. 2047, at ¶ 88 (Delhi High Court, Apr. 10, 2019) [hereinafter *UTV Software Communication*].

> e. whether the online location makes available or contains directories, indexes or categories of the means to infringe, or facilitate an infringement of, copyright;
> f. whether the owner or operator of the online location demonstrates a disregard for copyright generally;
> g. whether access to the online location has been disabled by orders from any court of another country or territory on the ground of or related to copyright infringement;
> h. whether the website contains guides or instructions to circumvent measures, or any order of any court, that disables access to the website on the ground of or related to copyright infringement; and
> i. the volume of traffic at or frequency of access to the website;
> j. Any other relevant matter.[119]

This is not to say that this multi-factor test is now expressly used in all Indian cases. As with courts in other jurisdictions, an Indian judge may simply determine, after reviewing the evidence, that the online locations in question are "rogue websites."[120] In subsequent cases, Indian judges have granted site-blocking orders against websites that are judged to be "new iterations of domains/websites that were earlier blocked";[121] that ignored notices to cease infringements;[122] whose "glaring features" included hidden identities of ownership or management;[123] and that "ask[ed] viewers or users to suggest more content that could be uploaded"[124] which the court considered to be "welcoming viewers to suggest more and more titles that can be unauthorizedly made available."[125] Of course, all these evidentiary elements fit within the *UTV Software Communication* framework.

---

119. *Id.* at ¶ 59. The court noted that this list was illustrative and not exhaustive. *Id.* at ¶ 60.

120. Universal City Studios v. Vegamovies.run, CS(COMM) 265/2022 and I.A. 14120/2023, 14122/2023 at ¶ 10 (Delhi High Court, April 27, 2022), https://indiankanoon.org/doc/106006995/ [https://perma.cc/99JL-NWEK].

121. *Id.* at ¶ 18. The court added that "[e]vidence collected by the investigator shows that the operators of the Defendant Websites are using known 'pirate branding' to signal to users that the Defendant Websites are merely new iterations of sites that have been blocked earlier." *Id.*

122. *Id.* at ¶ 19.

123. Universal City Studios v. Dotmovies.baby, (2023) CS(COMM) 514/2023 and I.A. 14120/2023, 14122/2023, at ¶ 8(i)–(iii) (Delhi High Court, Aug. 9, 2023).

124. *Id.* at ¶ 8(iv).

125. *Id.* at ¶ 8(iv).

V. RIGOROUSLY IDENTIFYING BAD GUYS AMELIORATES OTHER CONCERNS

Once past the obvious cases of self-proclaimed "pirate bays," clarity about the kinds of online locations subject to blocking orders can give us greater confidence that site-blocking for copyright enforcement will not have a significant, adverse impact on freedom of expression. Going forward, decisionmakers should have a clear list of factors for determining whether a site merits blocking, particularly if representatives of that online location are not before the court. The different evidentiary elements considered by legislatures and courts to date actually form a set of factors and what might be called "meta-factors."

A. Purpose and/or Predominant Use

No question for determining site blockage is more important than a finding that the site's purpose and/or predominant use is unauthorized distribution or unauthorized making available of copyrighted works. Indeed, this factual determination is *definitional:* it is effectively *the* determination whether the site is a "rogue website," "pirate website," or "flagrantly infringing online location."

Should the plaintiffs be required to establish that the targeted online location has copyright infringement as its *purpose*? Or should it be sufficient that to show that the online location is being *used predominantly* (or perhaps almost exclusively) for infringement? One can prefer the former as providing a more principled net to catch only bad actors.[126]

But we can expect that platforms launched as infringement-based business models will only sometimes admit that. If anything, they have incentives to do the opposite, i.e., to profess legal compliance and tell internet users what they offer only in terms of "choice," "variety," "freedom," low costs, and ease of use.[127]

---

126. Foong & Gray give the example of cyberlockers. Foong & Gray, *supra* note 11, at 365 ("Australia does not need a separate ground of primary effect of infringing or facilitating such infringement in [section] 115A, and 'primary purpose' alone as set out in the pre-2018 version of the regime is sufficient."). Foong & Gray give the example of cyberlockers as services that may be used principally for infringement but were not intended for that purpose. *Id.* at 356.

127. *See, e.g.*, *Roadshow Films Pty Ltd v Telstra Corp Ltd* [2020] FCA 507 [59] [hereinafter *Roadshow III*] ("Many of the streaming and linking target online locations provide statements which: claim they are in compliance with copyright; disclaim their liability for any infringing content; and/or provide instructions to teach users how to access infringing content."); *Roadshow Films Pty Ltd v Telstra Ltd* [2024] FCA 485 [28] [hereinafter *2024 Roadshow Films*] ("Many include statements about copyright compliance, claiming to have

In such an environment the distinction between predominant *purpose* and predominant *use* may also be more theoretical than practical as courts often *infer* the purpose of an online location from *how it is being used*. For example, in its 2018 *Disney Enterprises v. M1 Limited* decision, the Singapore High Court concluded the following:

> [T]he primary purpose of the websites . . . to commit or facilitate copyright infringement . . . was evident from the fact that searches for cinematograph films on the 53 websites disclosed a large number of page results, and a significant number of the Subject Films were made accessible through the websites without the consent or authorisation of the respective copyright owners.[128]

The websites in question were pirate streaming websites, P2P websites, and linking websites ("that contain[ed] an index of hyperlinks to copyrighted films which redirects the end-user to the hyperlinked site").[129]

Similarly, in the Australian 2016 *Roadshow Films v Telstra* decision, the SolarMovie website provided an unauthorized streaming service with over 15,000 motion pictures and over 138,000 television episodes,[130] causing the court to conclude that "the primary purpose of the SolarMovie website was to infringe or to facilitate the infringement of copyright in cinematograph films."[131] A subsequent Australian decision interpreted the statutory "purpose" requirement of Section 115A as "direct[ing] the Court to consider the principal activity for

---

copyright, yet they offer large catalogues of infringing material, and most of them make money by displaying advertising to users."); *Foxtel Mgmt Pty Ltd v TPG Internet Pty Ltd* [2017] FCA 1041 [55–56] [hereinafter *Foxtel Management 2017*] (noting "We take copyright violation very seriously" posted at site that did not respond to notices).

128. *Disney Enterprise*, *supra* note 37, at ¶ 9; *id.* at ¶ 25 ("The plaintiffs adduced sufficient evidence that the main purpose of all 53 websites was to commit or facilitate copyright infringement by showing, *inter alia*, that the websites provided access to a large library of films, including the Subject Films, without the authorisation of the owners of the copyright."); *id.* at ¶ 26 ("[O]perators of the websites demonstrated a disregard for copyright generally by virtue of the extent of the copyright infringement . . . .").

129. *Disney Enterprises*, *supra* note 37, at ¶ 24. The linking sites included links to sites providing subtitles of audiovisual works.

130. *Roadshow I*, *supra* note 34, at ¶ 65–68.

131. *Id.* at ¶ 69; *id.* at ¶ 74 ("In particular, I am satisfied that the SolarMovie website was designed and operated to facilitate easy and free access to cinematograph films made available online, something which, I would infer, has almost certainly occurred without the permission of the owners of the copyright in such films.").

which the online location exists and the principal intention of users of that online location."[132]

It is also worth pointing out that these injunctions have consistently been directed at websites that are dedicated to the *facilitation* of infringement. Courts have rejected the argument that sites which provide only links or torrents to third-party sources are themselves neither distributing nor making available.[133]

If the measure is descriptive — how the website is used — and not intentional — the purpose for which the website is operated — how "predominant" must the infringing activity be? The standard should be an "intentionally high threshold"[134] that filters out platforms that have only modest or moderate amounts of infringement relative to their overall activities. But it should not be too high. Early Indian blocking orders were focused on enforcing copyright for a single film and focused on URLs where the work could be found,[135] but subsequent Indian decisions have blocked websites, requiring only that what is available on a website be overwhelmingly infringing material.[136]

A bill introduced in the U.S. Congress in early 2025 to expressly authorize site-blocking injunctions also shows this melding of purpose and predominant use.[137] While H.R. 791 may be only a starting point for development of legislation in the United States, its provisions are

---

132. *Universal Music Australia Pty Ltd v TPG Internet Pty Ltd* [2017] FCA 435 [19] [hereinafter *Universal Music Australia*] ("[Section] 115A(1)(c) requires that the primary purpose of the online location is to infringe, or facilitate the infringement of, copyright (whether or not in Australia). . . . The primary purpose test directs the Court to consider the principal activity for which the online location exists and the principal intention of users of that online location."). *See also Foxtel Management Order 2018*, *supra* note 73, at ¶ 21.

133. *See, e.g.*, *Disney Enterprises*, *supra* note 37; Paramount Home Ltd v. British Sky Broadcasting Ltd [2014] EWHC 937 (Ch); 1967 Ltd v. British Sky Broadcasting Ltd [2014] EWHC 3444 (Ch) [14] ("It was immaterial that users of 13 of the Target Websites obtained the torrent files from third party websites by clicking on links provided by those Target Websites, rather than directly from the Target Websites themselves."); Case C-610/15, StichtingBrein v Ziggo, ECLI:EU:C:2017:456, ¶ 45 (June 14, 2017) (holding that the well-known user submitted link/torrent The Pirate Bay website directly infringes copyright in the European Union).

134. House Explanatory Memorandum (Austl.), at ¶ 6 (the goal is to "set an intentionally high threshold test for satisfaction by the Court. The purpose of the scheme is to allow a specific and targeted remedy to prevent those online locations which flagrantly disregard the rights of copyright owners from facilitating access to infringing copyright content").

135. Eros Int'l Media Ltd. v. Bharat Sanchar Nigam Ltd., (2015) 919 NMSL 3511, at ¶ 4(a)(iii) (Delhi High Court); Eros Int'l Media Ltd. v. Bharat Sanchar Nigam Ltd., (2016) 904 NMSL 1680, at ¶ 5(a)(iii) (Delhi High Court).

136. Dep't of Elecs. & Info. Tech. v. Star India Pvt. Ltd., (2015) FAO(OS) 57/2015, at ¶ 13 (Delhi High Court, July 29, 2016); *UTV Software Communication*, *supra* note 118. The *UTV Software* court noted, "that if the test to declare a website as a rogue website is that it should contain only illicit or infringing material, then each and every rogue website would add a small percentage of legitimate content" *Id.* at ¶ 68.

137. Foreign Anti-Digital Piracy Act, H.R. 791, 119th Cong. (2025). The bill was introduced by Representative Zoe Lofgren, the ranking Democrat on the Intellectual Property Subcommittee of the House Judiciary Committee.

instructive. In order to issue an injunction, the court must find that the website or online service to be blocked:

> (i) is primarily designed or primarily provided for the purpose of infringing copyright;
> (ii) has no commercially significant purpose or use other than infringing copyright; or
> (iii) is intentionally marketed by or at the direction of the operator of the foreign website or online service to promote the use of the website or online service in the infringement of copyright.[138]

We can reasonably understand "(i)" and "(iii)" as "purpose" tests, while "(ii)" — no other commercially significant use beside infringement — goes directly to how the website is being used.

Given the usual lack of more direct evidence, courts have (and *should*) use a variety of factual determinations to *strengthen* the *inference* that an online location is a rogue website. Courts have often treated these factors as distinct, but the various factors are actually all in the service of proving the website's piratical purpose. (As discussed above, Australia and Singapore have built many of these factors into their statutory law.)[139]

1. Indexes, Guides, Directories, or Categorization that Abets Infringement

Generally speaking, if an online location is organized in a way that seems to intentionally make unauthorized access to copyrighted works easier, that organization should serve as evidence of the website's purpose and/or predominant use. Such structural elements include categorization, directories, or indices ("comedy," "drama," "telenovelas," "scifi"),[140] pre-designated search terms ("Beyonce,"

---

138. *Id.* at § 502A (a)(2)(E).

139. The early 2025 legislative proposal in the U.S., House Bill 791, does not. *Id.*

140. Newzbin1 had categories for "Anime," "Apps," "Books," "Consoles," "Games," "Movies," "Music," with the "Movies" category further broken down into subcategories "indicative of piracy." *Newzbin2*, *supra* note 33, at ¶ 33. Its successor, Newzbin2, had the same categories. *Id.* at ¶ 48; *see also UTV Software Communication*, *supra* note 118, at ¶ 8 (noting websites in question "provide searchable indexes along with curated lists of top movies, television shows etc"); *id.* at ¶ 70 ("[Websites] contain indexes of the films, which are categorised including by quality, genre, viewership and ratings."); Dramatico Ent. v. British Sky Broadcasting [2012] EWHC 268 (Ch) [75(i)] [hereinafter *Dramatico Entertainment*] ("[Pirate Bay] indexes and arranges torrent files . . . to assist [users] in browsing for content to download."); *Universal Music Australia*, *supra* note 132, at ¶ 74 ("The online location allows users to search for content using terms such as '*CD rip*', '*DVD rip*' and '*iTunes rip*'."); *Roadshow Films Pty Ltd v Telstra Corp Ltd* [2017] FCA 965 ¶ 36–

"Prince," "Southpark") and guides to use of the online location that clearly indicate the website operators are aware of and condone infringing activity.[141] At the same time, it should be noted that such directories or indices can be machine-generated (and this will likely become more common), so, again, *some meaningful* operator decision(s) or participation in establishing the structural elements is important.

2. Evading Enforcement

Actions by operators of the alleged rogue website(s) to evade copyright enforcement, such as small changes in domain names or URLs that frustrate blocking, should serve as evidence of the website operators' purpose and intent.[142] The same when the operators of the alleged rogue website(s) provide guidance to their users on how to evade copyright enforcement.[143] Obviously, if the website operators engage in evasive efforts to continue to provide their services, this is both a bad guy indicium and a reason for dynamic injunctive relief.[144]

---

38 [hereinafter *Roadshow II*]; *Roadshow III*, *supra* note 127, at ¶ 29 ("[A] user is often presented with the option to select featured content such as 'New TV Shows' or 'Popular Movies . . . .'"); *id.* at ¶ 48 ("The website offers users the option to 'select a category' such as "Movies', 'Games', 'Software'. and 'Music'."); *id.* at ¶ 63 (describing website where "[c]ontent is frequently categorised under headings such as 'Latest Episodes', 'Popular Anime' and 'Top Dubbed'"); *2024 Roadshow Films*, *supra* note 127, at ¶ 27 ("[Websites] have directories, indexes or categories of motion pictures and television programs."); *Foxtel Management 2017*, *supra* note 127, at ¶ 58 (discussing a "genre" drop down menu with "action", "family", "horror", etc. categories); *Id.* at ¶ 93 (noting the website homepage had a menu bar with options including "Movies", "TV Series", "New Episodes", "Genre" and "Country").

141. *Universal Music Australia*, *supra* note 132, at ¶ 74 ("The online location provides explanations for how to use the site, how to upload content for other users to download by means of the BitTorrent protocol, and provides a mechanism for users to request that particular content be uploaded and made available free of charge."); *Roadshow II*, *supra* note 140, at ¶ 38 (noting websites included "information instructing users how to upload, view or download unauthorized copyright materials").

142. *Universal Music Australia*, *supra* note 132, at ¶ 24 ("The Nominated Domain Names in the amended pleadings reflect domain names which, phoenix-like, have appeared online as the means by which the KAT website may now be accessed by users following the closure of access to the Original Domain Names."); *Roadshow III*, *supra* note 127, at ¶ 74.

143. *See, e.g.*, *UTV Software Communication*, *supra* note 118, at ¶ 70 ("Instructions to circumvent measures taken to disable access were also found on a number of these websites, as evidenced by screenshots of posts, which show the owner or operator of the websites informing users of a change of domain name for the websites."); *Disney Enterprises*, *supra* note 37, at ¶ 26 ("Instructions to circumvent measures taken to disable access were also found on a number of these websites, as evidenced by screenshots of posts on these websites, which show the owner or operator of the websites informing users of a change of domain name for the websites."); *Roadshow II*, *supra* note 140, at ¶ 40 ("[Websites] include notices encouraging users to implement technology to frustrate any legal action that might be taken by copyright owners.").

144. *See, e.g.*, *Teksavvy*, *supra* note 35, at ¶ 81 ("Teksavvy notes that the Order has had to be updated several times to meet the defendants' reactions to it.").

3. Non-Responsiveness to Infringement or Legal Notices

Disregard for a plaintiff's takedown notices, cease-and-desist letters, and other communications to address the infringing activities should serve as evidence of an alleged rogue website operators' purpose and intent.[145] This should include *pro forma* automated responses on the part of the operators that make little or no sense and have no active follow-up.[146] In Germany, the non-responsiveness of the alleged rogue websites appears to be a justificatory foundation for blocking orders against ISPs.[147]

When there is absolutely no response from the website operator, to make this kind of inference, it is important that the court conclude that the website operators received the plaintiff's communications and that those communications both provide adequate information about the alleged infringing activity and give the website operators adequate time to respond.[148] The notices or cease-and-desist demands must have been "reasonably calculated" to reach the website operators.[149]

To the degree that the website operators *cannot be identified or located*, strictly speaking this kind of inference of the website operators' purpose (*there was notice, then no response*) cannot be made. In such circumstances, the court should be able to dispense with

---

145. *See, e.g.*, Cartier Int'l AG v. British Sky Broadcasting Ltd [2014] EWHC 3354 (Ch) [198] (describing cease-and-desist letters sent "to the named registrants of the domain names as identified by a WHOIS search. Unsurprisingly, these letters were simply ignored."); *Disney Enterprises*, *supra* note 37, at ¶ 26 ("[O]perators of the websites demonstrated a disregard for copyright generally by . . . non-compliance with the take-down notices issued by the plaintiffs."); *Foxtel Management Order 2018*, *supra* note 73, at ¶ 10.

146. *Universal Music Australia*, *supra* note 132, at ¶ 41 (noting that website operators sent automated replies that were "pro forma, inaccurate, and, in my view, not a proper response to a serious complaint"); *id.* at ¶ 44 ("[A]n obviously non-responsive and irrelevant response was received . . . . In any event, no substantive response was received."); *Roadshow II*, *supra* note 127, at ¶ 23 ("In each case the operators: (a) did not respond, (b) provided a non-responsive or evasive response, or (c) the email address was not operational."); *2024 Roadshow Films*, *supra* note 127, at ¶ 31–32 (describing no or automated responses from websites).

147. Frosio & Bulayenko, *supra* note 7, at 1132 ("In particular, according to German courts, there must be no alternative option or no way to reach the infringer himself directly, who must not have responded to the request to cease the infringing conduct. In sum, German courts require the order to be an 'ultima ratio' as a requirement for issuing a blocking injunction.").

148. Parallels can be drawn to due process jurisprudence on adequacy of notice. Mullane v. Cent. Hanover Bank & Tr. Co., 339 U.S. 306, 314 (1950) ("The notice must be of such nature as reasonably to convey the required information, and it must afford a reasonable time for those interested to make their appearance."); *id.* at 315 ("The means employed must be such as one desirous of actually informing the absentee might reasonably adopt to accomplish it.").

149. *Mullane*, 339 U.S. at 314; *see also* United Student Aid Funds, Inc. v. Espinosa, 559 U.S. 260, 272 (2010); Volkswagenwerk Aktiengesellschaft v. Schlunk, 486 U.S. 694, 707 (1988) (applying "reasonably calculated" standard to foreign defendants and concluding "the Due Process Clause does not require an official transmittal of documents abroad every time there is service on a foreign national").

any notice requirement.[150] As discussed below, inability to provide notice because of apparent efforts by the website operators to remain anonymous or unlocatable serves as a distinct justification for the blocking order.

B. Intentional Website Owner or Operator Anonymity

Efforts made by the owners or operators of the online location to remain anonymous, unidentified, and unidentifiable can be another indicium of a bad actor.[151] Alone, such efforts may evince nothing more than a desire for privacy, but when combined with other evidence, an adjudicator may reasonably conclude that use of tools to maintain anonymity or providing false data to avoid being identified indicates a party consciously avoiding the law. In the *Newzbin2* case, Justice Arnold quoted a spokesperson for the rogue website who had publicly said that the site was operated by a "small team of digital highwaymen who, thank you, prefer to remain behind their face-masks."[152]

Usually, evidence of efforts to remain anonymous is less colorful, but still systematic. In the 2021 *TekSavvy Solutions* decision,[153] the Canadian trial court judge noted the defendants' "obvious efforts to remain anonymous and avoid legal action by rightsholder such as the Plaintiffs."[154] The appellate panel endorsed the view of irreparable harm to the plaintiffs where there was "ongoing copyright infringement by defendants who are anonymous, and who are making clear efforts to remain so and avoid liability."[155] In the 2022 *DirectTV Argentina* case, the Buenos Aires court considered the plaintiff's allegations that the defendant websites used a tool allowing "those responsible to take

150. *Universal Music Australia*, *supra* note 132, at ¶ 37 ("[I]f the Court is satisfied that the owner of the copyright is unable, despite reasonable efforts, to determine the identity or address of the operator, or to send notices to that person, the Court may dispense with notice on such terms as it sees fit."); *id.* at ¶ 38 (dispensing with notice "on the basis that the applicants have been unable, despite reasonable efforts, to determine the identity or address of the person who operates the online location"); *Roadshow III*, *supra* note 127, at ¶ 25 (deciding that after "reasonable efforts to determine the identity of, and to contact in order to provide relevant notice of these proceedings," the court was "satisfied that it is appropriate to dispense with the notice requirement").

151. *Dramatico Entertainment*, *supra* note 140, at ¶ 12 (noting that The Pirate Bay operators could not be located); *UTV Software Communication*, *supra* note 118, at ¶ 70 ("[T]he infringing nature of the defendants' websites is apparent from the fact that their WHOIS detail is masked and no personal or traceable detail is available either of the Registrant or of the user."); *id.* at ¶ 71(a).

152. *Newzbin2*, *supra* note 33, at ¶ 56.

153. *TekSavvy*, *supra* note 35, at ¶ 1, (repeating Bell Media Group, et al. v. John Doe 1 dba GoldTV.biz, Order and Reasons, 2019 FC 1432 at ¶ 7).

154. *Id.* at ¶ 71 (quoting ¶ 7 of the trial court order).

155. *Id.* at ¶ 71; *see also id.* at ¶ 85 ("undisputed finding that the defendants make efforts to remain anonymous").

refuge in anonymity and/or enter false data to avoid being identified."[156]

C. Decisions of Other Courts

Perhaps the most interesting factor on the three lists in Part IV — and often discussed by other courts — is orders from courts of other jurisdictions either disabling access to the target websites or finding those target websites directly liable. Judges in numerous countries have been comfortable citing this as evidence supporting blocking injunctions in their own jurisdiction. This seems to occur especially within juridical "families," as when Nordic courts recognize what has happened in other Nordic jurisdictions[157] or common law courts recognize what has happened in other common law countries.[158] As blocking orders have increased globally, there may be more of this "cross-referencing."[159]

Critics may point out that this risks circular reasoning or a domino effect: site-blocking in one jurisdiction will contribute to the next jurisdiction ordering site-blocking, which will contribute to the next jurisdiction ordering site-blocking, and so on. But the willingness of jurists to accept this sort of evidence also shows how much jurists implicitly assume that copyright's legal norms are roughly harmonized across borders. For many of us, judges citing the decision of courts in other jurisdictions as providing support for their own conclusions can also be taken as a positive development for the rule of law globally.[160]

---

156. *See, e.g.*, *DirectTV Argentina*, *supra* note 36 (alleging that online locations used "herramientas informáticas propias del entorno digital que permite que los responsables se amparen en el anonimato y/o consignen datos falsos para evitar ser identificados").

157. In its 2010 decision upholding a site-blocking order against The Pirate Bay, the Danish Supreme Court noted that The Pirate Bay's leaders had already been criminally convicted of contributory copyright infringement in Sweden. Telenor v. IFPI (MDT2), decision of 27 May 2010, English translation available at http://hssph.net/Sonofon_IFPI__DK_SupremeCourt_27May2010_PirateBay.pdf; *see also* Finnish National Group of IFPI v. Elisa Oyj, District Court of Helsinki, H 11/20937, Judgment 11/41552 (26 October 2011) (citing that The Pirate Bay leaders "were convicted of aiding and abetting copyright infringement in the Royal Court of Sweden").

158. *Disney Enterprises*, *supra* note 37, at ¶ 27; *Roadshow III*, *supra* note 127, at ¶ 47–48 (noting blocking in other jurisdictions, including by UK High Court); *UTV Software Communication*, *supra* note 118, at ¶ 71(e) (observing that the "rogue nature of these websites has already been accepted by courts in other jurisdictions such as in Australia").

159. *Universal Music Australia*, *supra* note 132, at ¶ 76 ("The KAT website has already been the subject of orders blocking access to it on the basis of copyright infringement in a '*significant number of jurisdictions*', including the United Kingdom, Ireland, Denmark, Italy, Finland and Belgium."); *2024 Roadshow Films*, *supra* note 127, at ¶ 30 ("[A]t least six of the Target Online Locations are the subject of orders from a Court in another country on the ground of, or on grounds related to, copyright infringement.").

160. *See generally* Justin Hughes, *The Charming Betsy Canon, American Legal Doctrine, and the Global Rule of Law*, 53 VANDERBILT J. TRANSLATIONAL L. 1147 (2020); STEPHEN BREYER, THE COURT AND THE WORLD 91 (2016).

VI. JUSTICE AND EFFICIENCY IN DYNAMIC INJUNCTIONS

Dynamic injunctions accentuate free expression concerns. Since the entire idea of a "dynamic" or "adaptive" injunction is to increase speed and efficiency by reducing judicial processes, there will invariably be *some* reduction in the procedural safeguards for free expression provided by courts.

At the same time, concerns about dynamic injunctions should not be overblown. A proper dynamic injunction, in the words of the Singaporean court, "only requires the [ISPs] to block additional domain names, URLs and/or IP addresses that provide access to the same websites which are the subject of the main injunction."[161] But the "same website" needs to include minor changes (particularly some such changes to avoid enforcement), *de facto* equivalent content and functionality,[162] and/or purposeful "brand" imitation of popular piracy website domain names.[163] Anything beyond those categories fits less comfortably within the framework of an expedited dynamic injunction process.

The "dynamic" extension of a site-blocking injunction should still be within some specific parameters:

(1) Obviously, there must be written notice of the sought extension to the ISPs, the new target online locations,[164] and the courts; such notice should identify the domain names, URLs, and IP addresses to be added to the blocking order;[165]

(2) Such an extension notice should "stat[e] that the applicants have the good faith belief that the website operated at the different domain name, IP Address or URL is a new location for the target online locations that are already the subject of the orders;"[166]

---

161. *Disney Enterprises*, *supra* note 37, at ¶ 38.

162. On these two points, the bill introduced in the U.S. Congress in 2025 would allow for the amendment of injunctions to add "additional domain names or internet protocol addresses" if the court determines that the blocked website is accessible in its original or "reconstituted" form through those channels or if the blocked website "has engaged in circumvention techniques that render the initial order ineffective." Foreign Anti-Digital Piracy Act, H.R. 791, 119th Cong. § 502A(b)(4)(A)(B) (2025).

163. IP HOUSE, *supra* note 104, at 31 (noting courts in Australia, India, and the UK issue "brand orders" against "copycat sites that intentionally use domain names similar to popular piracy sites in order to encourage user traffic.").

164. This will often have to be good faith attempts to provide notice, as the pirate sites often seek to prevent communications.

165. *See, e.g.*, *Roadshow III*, *supra* note 127, at ¶ 72(1).

166. *Id.*

(3) The extension notice should, as filed with the court, constitute an affidavit as to the facts made under penalty of perjury;[167]

(4) The ISPs should be given an opportunity to object,[168] but the timeframe for their implementation of the extended blocking and the timeframe for ISP objection need not be the same;

(5) If there is such an objection from an ISP, then the court needs to schedule a hearing in relation to that ISP;[169]

(6) There should be an appropriate penalty for *fraudulent* or *deceptive* use of the dynamic injunction mechanism to any domain names, URLs, or IP addresses that do *not* provide access to the same websites or equivalent content as are the subject of the main injunction, such as unwinding the original injunction in its entirety, i.e., a penalty that impacts the copyright owner directly and not just counsel;

(7) All site-blocking injunctions, including dynamic ones, should have a sunset provision.[170]

The goal of jurisdictions adopting this type of framework — whether by persuasive court decisions or legislative codification — should be to have efficient, adaptive extension of site-blocking orders without significant increasing risks to freedom of expression.

VII. CONCLUSION

The internet environment continues to evolve, and evolution produces malignant mutations at least as often as it produces beneficial ones. As Rogers Brubaker put it, our early internet "dreams of digital democracy and the sharing economy" have been "curdling into a nightmare of polarization and 'platform capitalism.'"[171] This capitalism includes infringement-based business models[172] that not only ignore

167. For example, this is part of the DMCA's take-down notifications, but only as to whether "the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed." 17 U.S.C. § 512(c)(3)(vi).

168. *See, e.g.*, *Roadshow III*, *supra* note 127, at ¶ 72(2).

169. *Id.* at ¶ 72(3).

170. Perel, *supra* note 62, at 46.

171. Rogers Brubaker, *Hyperconnected Culture and Its Discontents*, NOEMA (Jan. 3, 2023), https://www.noemamag.com/hyperconnected-culture-and-its-discontents/ [https://perma.cc/Z257-7STR].

172. *See, e.g.*, *Newzbin2*, *supra* note 33, at ¶ 30 ("In the year ending 31 December 2009 Newzbin Ltd had a turnover in excess of £1 million and a profit in excess of £360,000."); *Dramatico Entertainment*, *supra* note 140, at ¶ 29 (estimating The Pirate Bay to have conservatively made "US$ 1.7 to 3 million" in revenue for one month in 2011); *UTV Software Communication*, *supra* note 118, at ¶ 51 (citing revenue calculations for The Pirate Bay from Swedish prosecutors and for KickAss Torrents from U.S. law enforcement).

copyright but also generally prove immune to law enforcement. By enlisting the ISP "elephants" against these actors, access denial emerged as a cost-effective method of reducing copyright infringement.

With questions about technical ability and burden-sharing largely worked out, the potential impact of site-blocking on free expression remains. This is a legitimate concern, although little or no significant adverse impact from judicially-supervised site-blocking has yet been demonstrated empirically and policymakers will never satisfy all those who express concern for free expression because some are opposed to copyright enforcement, *period*. For those genuinely seeking a balance between internet users' free expression and copyright owners' interests, site-blocking regimes should have express criteria for identifying online locations that merit blocking — whether we call them "rogue websites," "flagrantly infringing online locations," or just bad guys.