

78015 - Global Aspects of Intellectual Property Law - Summer 2025

24715841

Global Aspects of Intellectual Property Law

Research Essay

A. Introduction

Online copyright infringement is now predominantly facilitated through digital networks.¹ Direct enforcement against individual users is often costly and difficult to scale, which has shifted regulatory attention toward intermediaries, particularly internet service providers (ISPs), as they control technical chokepoints and hold key evidence and identity pathways.² This institutional response creates a predictable tension, as enforcement tools often incentivise collection, retention, and disclosure of user data, bringing copyright policy into direct contact with privacy law and human rights norms.³

This essay evaluates the effectiveness of international intellectual property instruments, particularly the WIPO Internet Treaties, in shaping ISP liability regimes for online copyright infringement while respecting user privacy rights.

Effectiveness is assessed using three criteria. First, coherence and predictability consider whether the framework meaningfully guides stable models across states or leaves key architecture open. Second, enforcement workability tests whether regulatory measures function at an internet scale without incentivising overreach. Third, rights compatibility asks whether privacy safeguards are embedded in domestic law and effectively enforced by the judiciary.

The central assertion is that while the WIPO Internet Treaties (**WCT/ WPPT**) establish the digital rights baseline and supporting obligations (TPMs/RMI),⁴ and *TRIPS* sets general expectations for effective enforcement,⁵ neither instrument meaningfully constrains how enforcement is implemented through intermediaries, nor resolves the tension between effective enforcement and the protection of user privacy.⁶ As a result, effectiveness is largely realised (or fails) downstream through domestic legislative design and

¹ Department of Communications, *Online Copyright Infringement Research: A Marketing Research Report* (Report, TNS Australia, 24 June 2015) 8-9 ('*Online Copyright Infringement Research*').

² Joshua Gacutan and Niloufer Selvadurai, 'The Relevance of Internet Architecture to Law: The Liability of Internet Service Providers for Harmful User-Generated Content' (2022) 3(1) *Australian National University Journal of Law and Technology* 55, 56-58.

³ *Privacy Act 1988* (Cth); *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17 ('*ICCPR*').

⁴ *WIPO Copyright Treaty*, opened for signature 20 December 1996, 2186 UNTS 121 (entered into force 6 March 2002) arts 8, 11-12 ('*WCT*'); *WIPO Performances and Phonograms Treaty*, opened for signature 20 December 1996, 2186 UNTS 203 (entered into force 20 May 2002) arts 10, 14, 18-19 ('*WPPT*') (collectively '*WIPO Internet Treaties*').

⁵ *Agreement on Trade-Related Aspects of Intellectual Property Rights*, opened for signature 15 April 1994, 1869 UNTS 299 (entered into force 1 January 1995) art 41 ('*TRIPS*').

⁶ *TRIPS* (n 5) arts 41(1), 41(5); *WCT* (n 4) arts 8, 11-12; *WPPT* (n 4) arts 10, 14, 18-19.

court-managed proportionality and disclosure control, producing fragmentation and shifting compliance pressure onto intermediaries.⁷

B. International Instrument Standardisation

(i) TRIPS (Part III enforcement)

The Agreement on Trade-Related Aspects of Intellectual Property Rights (**TRIPS**) (a World Trade Organization (**WTO**) agreement setting minimum IP standards) requires Members to make enforcement procedures available that permit effective action against infringement and include safeguards against abuse. It also clarifies that Members are not obliged to establish a distinct judicial system for intellectual property enforcement. *TRIPS* further requires fair and equitable civil procedures for rights-holders, including access to civil judicial remedies. Members must also provide provisional measures to prevent infringement and preserve relevant evidence. *TRIPS* requires procedures that enable rights-holders to seek a customs suspension of suspected counterfeit and pirated goods. For serious infringement, criminal procedures and penalties are required, at least for wilful piracy and commercial-scale counterfeiting.⁸

However, *TRIPS* does not embed comprehensive constraints on the collection, retention, or disclosure of personal data in online enforcement, leaving proportionality and privacy safeguards to domestic law and broader human rights norms.⁹ It raises expectations of "effective action" while leaving safe harbours, notice systems, blocking, and disclosure processes to domestic law, as well as the design of any intermediary-facing enforcement measures.¹⁰ The result is limited cross-jurisdictional coherence in intermediary design, with rights compatibility largely contingent on domestic safeguards and judicial supervision.¹¹

(ii) WIPO Internet Treaties (WCT/WPPT)

The WIPO Copyright Treaty (**WCT**) and WIPO Performances and Phonograms Treaty (**WPPT**) (World Intellectual Property Organization (**WIPO**) "Internet Treaties") modernise

⁷ *Dallas Buyers Club LLC v iiNet Ltd* [2015] FCA 317 (‘*Dallas Buyers Club*’); *Roadshow Films Pty Ltd v Telstra Corporation Ltd* [2016] FCA 1503 (‘*Roadshow Films v Telstra*’).

⁸ *TRIPS* (n 5) arts 41, 41(5), 42, 50, 51, 61.

⁹ *Ibid* pt III; *ICCPR* (n 3) art 17; Organisation for Economic Co-operation and Development, *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (Report, 2011) (‘*OECD Report*’).

¹⁰ *TRIPS* (n 5) art 41; *OECD Report* (n 9).

¹¹ Global Commission on Internet Governance, ‘Intermediary Liability: Protecting Internet Platforms for Expression and Innovation’ (Paper No 42, CIGI and Chatham House, April 2016) 1-3; *OECD Report* (n 9); *Dallas Buyers Club* (n 7).

substantive rights for the networked environment by requiring protection for digital dissemination, including the “making available” aspect of communication rights.¹² The *WCT* requires Contracting Parties to provide authors with an exclusive right of communication to the public, encompassing on-demand online availability (“making available”).¹³ The *WPPT* mirrors this modernisation for neighbouring rights, extending the making-available style protection to performers and phonogram producers.¹⁴

The treaties are most prescriptive in two areas that indirectly support online enforcement. First, states must provide legal protection and effective remedies against circumvention of technological protection measures (**TPMs**), such as access/control locks (often DRM).¹⁵ Second, they require protection for rights management information (**RMI**) (metadata identifying ownership/terms), prohibiting specified knowing acts of removing or altering RMI and distributing works where RMI has been removed or altered.¹⁶ These obligations operate as anti-circumvention and anti-tampering rules that stabilise licensing and enforcement signals; they do not, in themselves, require intermediaries to engage in generalised inspection to detect infringement.¹⁷ Where automated detection arises in practice, it is most feasible for hosting platforms and services with content visibility, rather than for access providers to carry communications.¹⁸

For this essay, 'ISP' is used to broadly include access providers and, where relevant, hosting platforms subject to intermediary liability frameworks, while "ISP liability architecture" means the domestic model allocating responsibilities to intermediaries, including safe harbours, notice processes, blocking remedies, disclosure rules, and any monitoring-adjacent duties. Crucially, *WCT*/*WPPT* do not prescribe that architecture; they mandate neither notice-and-takedown nor blocking, and they impose no general monitoring model or disclosure standard. Their function is to set the rights baseline; the enforcement "plumbing" is left to domestic systems.¹⁹

¹² *WCT* (n 4) art 8; *WPPT* (n 4) arts 10, 14.

¹³ *WCT* (n 4) art 8.

¹⁴ *WPPT* (n 4) arts 10, 14.

¹⁵ *WCT* (n 4) art 11; *WPPT* (n 4) art 18.

¹⁶ *WCT* (n 4) art 12; *WPPT* (n 4) art 19.

¹⁷ Lilian Edwards, *Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights* (Report, World Intellectual Property Organization, 2011) 2.

¹⁸ Gacutan and Selvadurai (n 2) 55, 56-58.

¹⁹ Edwards (n 17); *WCT* (n 4) arts 8, 11-12; *WPPT* (n 4) arts 10, 14, 18-19.

C. ISP Toolkit

(i) Safe Harbour

Safe harbours are statutory limits on intermediary liability, designed to keep communications services functioning without making providers automatically responsible for user infringement.²⁰ For ISPs, the core category is "mere conduit" (and sometimes caching), reflecting limited visibility into content and the impracticality of general policing.²¹ Protection is conditional, typically requiring responsive compliance, such as adopting a policy for dealing with repeat allegations that links it to safe harbour, and cooperating with court orders, rather than a general duty to monitor.²²

(ii) Notice-based processes

Notice-based systems operationalise enforcement as notice-and-notice or notice-to-forward mechanisms where allegations are passed to subscribers to deter infringement and create a record.²³ These systems scale cheaply, but still create pressure toward over-compliance where intermediary risk is high.²⁴

(iii) Blocking injunctions

Blocking injunctions are court-supervised access restrictions aimed at online locations primarily dedicated to infringement (e.g., Australia's s 115A).²⁵ They are comparatively identity-light because they target access pathways rather than individual users.²⁶ Effectiveness depends on the method (DNS/IP/URL) and on managing circumvention and domain migration through updates or variations over time.²⁷ They raise questions of proportionality regarding over-blocking and cost allocation.²⁸

²⁰ Shahzeb Mahmood, 'Online Service Providers in Choppy Waters: Time to Revise Copyright Safe Harbour Scheme in Australia' (2023) 4(1) *Australian National University Journal of Law and Technology*.

²¹ Ibid 74-75.

²² Ibid 76-77.

²³ Ibid 146-147.

²⁴ Edwards (n 17); *OECD Report* (n 9) 144.

²⁵ *Copyright Act 1968* (Cth) s 115A.

²⁶ Justin Hughes, 'Comparative Online Bad Guys' (2024) 38(3) *Harvard Journal of Law & Technology* 603.

²⁷ Ibid; David Lindsay, 'Website Blocking Injunctions to Prevent Copyright Infringements. Proportionality and Effectiveness' (2017) 40(4) *UNSW Law Journal*.

²⁸ Lindsay (n 27) 1511.

(iv) Disclosure orders

Disclosure orders compel ISPs to identify subscribers associated with alleged infringement by linking observed activity, often IP address usage, to customer records.²⁹ The privacy stakes are heightened as enforcement hinges on data handling and compelled disclosure, with constraints generally derived from domestic privacy law and court-imposed limits on use, communication, and procedure.³⁰

(v) Retention

Retention and preservation records determine whether enforcement is even possible, as without logs, identity resolution fails.³¹ Privacy is entrenched here, as collection scope, retention periods, access controls, and secondary use limits determine how easily infringement allegations transfer into identification.³²

D. Privacy Collision

In this essay, privacy refers to data-protection governance over online user records, including the collection, retention, security, disclosure, and secondary use (including profiling) of subscriber and traffic-related data.³³ Privacy also includes the degree of identity linkability created by enforcement, and the desirability of protections against linking accounts or IP addresses to identifiable persons except where necessary and proportionate, consistent with baseline expectations under the Australian Privacy Principles and ICCPR art 17.³⁴

(i) Mechanism

To maintain privacy in proportion to the benefits of copyright enforcement, it is preferable to prioritise measures that can operate without identifying end users, such as court-supervised site-blocking, which targets access pathways to infringing online locations and is comparatively identity-light.³⁵ By contrast, serious deterrent or remedial

²⁹ *OECD Report* (n 9).

³⁰ *Dallas Buyers Club* (n 7).

³¹ *OECD Report* (n 9).

³² *Ibid.*

³³ *Privacy Act 1988* (Cth) sch 1 ('Australian Privacy Principles') (especially APP 3 (collection), APP 6 (use/disclosure), APP 11 (security)).

³⁴ *Ibid.*, *ICCPR* (n 3) art 17.

³⁵ *Copyright Act 1968* (Cth) s 115A; *Lindsay* (n 27); *Edwards* (n 17) 27-29.

pathways commonly depend on identity resolution and data handling.³⁶ Disclosure orders require an ISP to link observed network identifiers, typically IP address activity, to subscriber records.³⁷ Evidence preservation requires logs capable of connecting allegations to accounts over time.³⁸ Repeat-infringer logic, where tied to safe-harbour compliance or internal risk control, relies on persistent signals and record-keeping.³⁹ Accordingly, privacy friction is inevitable when enforcement relies on identity resolution, primarily because it relies on maintaining and analysing records that connect online activity to identifiable persons.

(ii) Scale

At the internet scale, individualised adjudication and one-off orders do not bear the primary enforcement burden, particularly where infringement is dispersed across large user bases and rapidly shifting online locations.⁴⁰ While site-blocking can reduce access to specific targets, it is vulnerable to mirror sites and rapid migration ("whack-a-mole"), and can be circumvented through VPNs and proxies.⁴¹ These limits can increase pressure to supplement identity-light remedies with scalable systems and automation, which, in turn, creates incentives for retention and preservation, monitoring pressure (including practices approximating monitoring), profiling and inference, automated detection and notice workflows, and intensified identity linkage across datasets.⁴²

E. Implementation Evaluation

(i) EU benchmark

The EU illustrates what enforceable "walls" look like in the context of intermediary enforcement. Limits are expressed as rules against generalised monitoring and as proportionality requirements grounded in fundamental rights.⁴³ The CJEU has rejected broad filtering obligations that would require intermediaries to conduct general monitoring,

³⁶ *Roadshow Films Pty Ltd v iiNet Ltd* [2012] HCA 16 ('*Roadshow Films v iiNet*').

³⁷ *Dallas Buyers Club* (n 7).

³⁸ Edwards (n 17).

³⁹ *OECD Report* (n 9); *Roadshow Films v iiNet* (n 36).

⁴⁰ Edwards (n 17) 26-29; *OECD Report* (n 9) 144-145; Tuomas Mylly, 'Proportionality in the CJEU's Internet Copyright Case Law: Invasive or Resilient?' in Sybe A de Vries and Ulf Bernitz (eds), [*General Principles of EU Law and the EU Digital Order*](#) (Wolters Kluwer, 2020) 267..

⁴¹ INCOPRO, *Site Blocking Efficacy: Key Findings — Australia* (Report, July 2018).

⁴² Mahmood (n 20); *OECD Report* (n 9) 145-149, 193; Edwards (n 17) 72.

⁴³ *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market* OJ L 178/1, art 15(1); *Charter of Fundamental Rights of the European Union* OJ C 326/391.

treating such measures as incompatible with rights-balancing where they are indiscriminate and risk blocking lawful content.⁴⁴ The DSM Directive's Article 17 increases platform responsibility and creates more substantial filtering incentives.⁴⁵ However, the CJEU upheld it only on the basis that safeguards that protect lawful content and preserve effective user redress.⁴⁶ For access-blocking, *UPC Telekabel Wien* confirms that blocking can be compatible when targeted and proportionate, aiming for "reasonable effectiveness", discouraging access rather than eliminating infringement, while leaving technical choices to ISPs.⁴⁷ The takeaway is that EU enforcement is legitimate only within explicit limits on general monitoring and within the discipline of proportionality, rather than through enforcement maximalism.

(ii) *Australia case study: domestic design and courts decide outcomes*

Australia implements treaty-aligned rights and general enforcement expectations primarily through the *Copyright Act*, while privacy protections are primarily found in the *Privacy Act 1988* (Cth) and the *Australian Privacy Principles*.⁴⁸ Because the *WIPO Internet Treaties* and *TRIPS* do not provide an intermediary liability architecture or privacy constraints, Australian outcomes turn on domestic design and judicial control.⁴⁹ This domestic 'plumbing' includes Australia's safe harbour scheme, which limits remedies for carriage service providers subject to conditions, but leaves the scope of any positive enforcement duties largely to statute and case law.⁵⁰ Courts serve as practical gatekeepers, determining whether their duties are imposed on intermediaries, supervising in proportion to the risk, and managing safeguards to prevent misuse of disclosure.⁵¹

(iii) *Roadshow Films Pty Ltd v iiNet Ltd*

⁴⁴ *Scarlet Extended SA v Société Belge des Auteurs, Compositeurs et Éditeurs SCRL* (Court of Justice of the European Union, C-70/10, ECLI:EU:C:2011:771, 24 November 2011); *SABAM v Netlog NV* (Court of Justice of the European Union, C-360/10, ECLI:EU:C:2012:85, 16 February 2012).

⁴⁵ *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] OJ L 130/92, art 17.

⁴⁶ *Republic of Poland v European Parliament and Council of the European Union* (Court of Justice of the European Union, C-401/19, ECLI:EU:C:2022:297, 26 April 2022).

⁴⁷ *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* (Court of Justice of the European Union, C-314/12, ECLI:EU:C:2014:192, 27 March 2014).

⁴⁸ *Copyright Act 1968* (Cth); *Privacy Act 1988* (Cth) sch 1.

⁴⁹ *TRIPS* (n 5); *WIPO Internet Treaties* (n 4).

⁵⁰ *Copyright Act 1968* (Cth) pt V div 2AA.

⁵¹ *Dallas Buyers Club* (n 7).

In *Roadshow Films*, the High Court refused to convert an access ISP into a general copyright enforcer by treating allegations and notice as sufficient to require termination or broad policing responses.⁵² The Court's approach reflects a reluctance to impose wide-ranging policing duties absent a clear legislative scheme, notably where the ISP lacks direct control over the infringing conduct and imposing obligations would shift significant enforcement burdens onto infrastructure providers.⁵³ The case supports the essay's claims of coherence and workability. Treaty baselines modernise rights, but they do not answer the domestic question of what an ISP must do in response to user infringement; domestic statute and common law determine that boundary.⁵⁴

(iv) Dallas Buyers Club LLC v iiNet Ltd

In *Dallas Buyers Club*, the Federal Court permitted preliminary discovery to identify account-holders associated with alleged BitTorrent activity, but treated disclosure as a high-risk enforcement step requiring strong anti-abuse controls.⁵⁵ Perram J was explicitly concerned about “speculative invoicing” dynamics (pressure to settle without adjudication) and, while discovery was available under the Court's procedural powers, the order was conditioned and effectively stayed pending safeguards. This included limits on the use of disclosed information and court supervision of any proposed correspondence to account holders. The decision illustrates that the treaties themselves do not deliver privacy and rights compatibility; they are implemented downstream through procedure, controlled disclosure, and judicial supervision designed to prevent coercive or misleading enforcement practices.

(v) s 115A + Roadshow Films Pty Ltd v Telstra Corporation Ltd

Australia's s 115A blocking regime further reveals domestic architecture shaping outcomes. Section 115A enables orders mandating carriage service providers to take reasonable steps to restrict access to online locations outside Australia whose primary purpose is to infringe or facilitate infringement of copyright, providing the Court explicit proportionality levers, including impacts on affected persons and public interest considerations.⁵⁶ In *Roadshow Films*, the Federal Court applied the provision to offshore

⁵² *Roadshow Films Pty Ltd v iiNet Ltd* [2012] HCA 16.

⁵³ *Ibid.*

⁵⁴ *Ibid*; *Copyright Act 1968* (Cth).

⁵⁵ *Dallas Buyers Club LLC v iiNet Ltd* [2015] FCA 317.

⁵⁶ *Copyright Act 1968* (Cth) s 115A.

piracy sites, illustrating how blocking channels enforcement toward a comparatively identity-light remedy that can be repeated and varied over time as domains migrate.⁵⁷ Technique choice matters, as DNS, IP, and URL blocking differ in cost and granularity, and therefore in overblocking risk and collateral impact; cost-allocation decisions can indirectly favour cheaper, coarser methods, shaping both effectiveness and rights footprint.⁵⁸

F. Evaluation

(i) Coherence and predictability

On coherence, the WIPO Internet Treaties and TRIPS are not designed to generate a single, predictable intermediary liability architecture, despite their effectiveness.⁵⁹ The gap is visible in the divergence of domestic “toolkits”.⁶⁰ States converge on protecting online dissemination and communication rights, yet vary sharply in how they implement enforcement through safe harbours, notice-based systems, blocking, and disclosure.⁶¹ This fragmentation is not accidental; it is the predictable consequence of treaty silence on intermediary architecture.⁶² The treaties provide a stable floor, while leaving the enforcement “plumbing” to domestic design choices.

(ii) Enforcement workability

Workability is therefore achieved downstream. Domestic tools can scale, but they do so by shifting operational burden onto intermediaries that control network chokepoints and information pathways.⁶³ Blocking can be deployed repeatedly and at a lower cost than end-user litigation, but it is vulnerable to migration and circumvention, which encourages systematised enforcement.⁶⁴ Where intermediaries have content visibility, automation improves scale but raises collateral risks by pushing toward monitoring-adjacent practices and over-removal.⁶⁵ The EU benchmark illustrates the distinction between scalable enforcement and scalable overreach, permitting blocking and heightened platform

⁵⁷ *Roadshow Films Pty Ltd v Telstra Corporation Ltd* [2016] FCA 1503.

⁵⁸ *Ibid*; *OECD Report* (n 9) 193; Edwards (n 17) 49.

⁵⁹ *TRIPS* (n 5); *WIPO Internet Treaties* (n 4).

⁶⁰ *OECD Report* (n 9) 143-156; Mylly (n 40) 267.

⁶¹ Edwards (n 17).

⁶² *Ibid*.

⁶³ Gacutan and Selvadurai (n 2) 55, 56–58.

⁶⁴ Lindsay (n 27).

⁶⁵ *Scarlet Extended SA* (n 44); *SABAM v Netlog* (n 44).

responsibility, but rejecting broad, indiscriminate filtering and insisting on proportionality discipline.⁶⁶

(iii) Rights compatibility (privacy)

Treaty-level privacy guidance is thin; accordingly, rights compatibility depends primarily on domestic safeguards and judicial supervision.⁶⁷ The collision is structural once enforcement relies on identity resolution and persistent signals. Disclosure, retention/preservation, and repeat-infringer logic all require data-handling practices that increase linkability risks and heighten the stakes of misuse.⁶⁸ Australia shows how courts manage the collision in practice, tightening preliminary discovery to prevent coercive "speculative invoicing" and funnelling enforcement toward comparatively identity-light blocking under s 115A with explicit proportionality mechanisms.⁶⁹ It relies on courts to set procedural ceilings through disclosure control and proportionality.

(iv) Counter-positions

A pro-enforcement objection is that baseline harmonisation remains genuinely effective. Minimum rights and enforcement expectations enable divergence as a feature, arguing that domestic systems are better placed to calibrate enforcement burdens and technological feasibility.⁷⁰ A pro-privacy objection exists because treaty silence systematically externalises privacy costs, as enforcement at scale predictably migrates to the entities holding data and chokepoints, regardless of formal legal duties.⁷¹ The best synthesis is that the instruments are effective as floors. However, they shape ISP liability and privacy outcomes only indirectly; the decisive ceilings, safeguards, and proportionality controls are supplied domestically, and often only through courts.⁷²

G. Conclusion

This essay responds that the WIPO Internet Treaties and TRIPS set a workable rights-and-enforcement floor but leave the architecture governing ISP duties and privacy outcomes to domestic law. In the intermediary setting, enforcement is inseparable from

⁶⁶ *Copyright in the Digital Single Market Directive* (n 45) art 17(4); *Poland v Parliament* (n 46) [50]; *UPC Telekabel* (n 47) [32].

⁶⁷ *Privacy Act 1988* (Cth); *TRIPS* (n 5) art 41; *WIPO Internet Treaties* (n 4); Edwards (n 17).

⁶⁸ *OECD Report* (n 9) 149-156; Edwards (n 17) 31-33.

⁶⁹ *Dallas Buyers Club* (n 7); *Copyright Act 1968* (Cth) s 115A; *Roadshow Films v Telstra* (n 7).

⁷⁰ *TRIPS* (n 5) arts 41-42, 50-51, 61.

⁷¹ Gacutan and Selvadurai (n 2) 56-58.

⁷² *Dallas Buyers Club* (n 7); *Roadshow Films v iiNet* (n 36); *Roadshow Films v Telstra* (n 7).

information power. Identification, retention, and disclosure become the operational currency of compliance. Effective regimes, therefore, require explicit domestic ceilings, clear limits on monitoring-adjacent practices, tightly controlled disclosure pathways, and proportionality as a hard constraint, as treaty-level direction is inadequate. By these metrics, treaty effectiveness is real but bounded, while domestic design determines the mechanism and the 'rights' costs.

BIBLIOGRAPHY

A. Articles/Books/Reports

Department of Communications and the Arts, *Online Copyright Infringement Research: A Marketing Research Report* (Report, TNS Australia, 24 June 2015)

Edwards, Lilian, *Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights* (Report, World Intellectual Property Organization, 2011)

Gacutan, Joshua and Niloufer Selvadurai, 'The Relevance of Internet Architecture to Law: The Liability of Internet Service Providers for Harmful User-Generated Content' (2022) 3(1) *Australian National University Journal of Law and Technology*

Global Commission on Internet Governance, 'Intermediary Liability: Protecting Internet Platforms for Expression and Innovation' (Paper No 42, CIGI and Chatham House, April 2016)

Hughes, Justin, 'Comparative Online Bad Guys' (2024) 38(3) *Harvard Journal of Law & Technology* 603

INCOPRO, *Site Blocking Efficacy: Key Findings — Australia* (Report, July 2018)

Lindsay, David, 'Website Blocking Injunctions to Prevent Copyright Infringements: Proportionality and Effectiveness' (2017) 40(4) *UNSW Law Journal* 1507

Mahmood, Shahzeb, 'Online Service Providers in Choppy Waters: Time to Revise Copyright Safe Harbour Scheme in Australia' (2023) 4(1) *Australian National University Journal of Law and Technology*

Mylly, Tuomas, 'Proportionality in the CJEU's Internet Copyright Case Law: Invasive or Resilient?' in Sybe A de Vries and Ulf Bernitz (eds), *General Principles of EU Law and the EU Digital Order* (Wolters Kluwer, 2020)

Organisation for Economic Co-operation and Development, *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (Report, 2011)

B. Cases

Dallas Buyers Club LLC v iiNet Ltd [2015] FCA 317

Republic of Poland v European Parliament and Council of the European Union (Court of Justice of the European Union, C-401/19, 26 April 2022)

Roadshow Films Pty Ltd v iiNet Ltd [2012] HCA 16

Roadshow Films Pty Ltd v Telstra Corporation Ltd [2016] FCA 1503

SABAM v Netlog NV (Court of Justice of the European Union, C-360/10, 16 February 2012)

Scarlet Extended SA v Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (Court of Justice of the European Union, C-70/10, 24 November 2011)

UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH (Court of Justice of the European Union, C-314/12, 27 March 2014)

C. Legislation

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391

Copyright Act 1968 (Cth)

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] OJ L 178/1

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] OJ L 130/92

Privacy Act 1988 (Cth)

D. Other (Treaties)

Agreement on Trade-Related Aspects of Intellectual Property Rights, opened for signature 15 April 1994, 1869 UNTS 299 (entered into force 1 January 1995)

International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976)

WIPO Copyright Treaty, opened for signature 20 December 1996, 2186 UNTS 121 (entered into force 6 March 2002)

WIPO Performances and Phonograms Treaty, opened for signature 20 December 1996, 2186 UNTS 203 (entered into force 20 May 2002)