Internet Intermediaries and Copyright – A 2018 Update

A policy paper produced for the Australian Digital Alliance

Professor Kimberlee Weatherall[1]

11 February 2018

Executive Summary

This paper was written at the request of the Australian Digital Alliance (ADA[2]) and updates an earlier policy paper which I wrote for ADA in 2011, titled *Internet Intermediaries and Copyright: An Australian Agenda for Reform*.[3] The 2011 paper reviewed Australian law relating to internet (online) intermediaries and their potential liability where their users engage in copyright infringement. That paper reviewed the law in Australia, the US, Canada, the EU (at the EU, but not national level), the United Kingdom, and New Zealand. It concluded that Australian copyright legislation imposed higher risks of liability on internet intermediaries than equivalent laws overseas, creating a comparative disadvantage for Australian-based educational and cultural institutions, businesses and others compared to their overseas competitors. It recommended that Australian law should be updated, including by expanding safe harbours found in Part V Div 2AA of the *Copyright Act 1968* (Cth).

In the six years since that paper, Australia has not altered its legislation, although expanding the availability of the safe harbours has been proposed in a 2014 Discussion Paper,[4] recommended by the Australian Productivity Commission,[5] and included in an earlier exposure draft of the Copyright Amendment (Disability and Other Access Measures) Bill.[6] Developments in Australian case law (discussed below) have made clear that the risks of liability for most internet intermediaries (beyond internet access providers) are real. There have also been developments overseas although, for the most part, they have not changed the fundamental position: comparable jurisdictions make safe harbours available to many internet intermediaries, in circumstances where Australian intermediaries – private and public – risk copyright liability.

Discussions of copyright law, especially intermediary liability, can be mind-numbingly complex, so the 2011 paper included a broad-brush table to illustrate how much risk an intermediary faced in different countries, using a 'traffic lights' approach: where *red* was used to indicate an activity

---

[1] Professor of Law, The University of Sydney Law School, The University of Sydney, and volunteer member of the Board of the Australian Digital Alliance. This paper was prepared at the request of the Australian Digital Alliance. Research assistance was provided by Mr Onur Saygin, paid by the Australian Digital Alliance. Professor Weatherall has received no financial benefit from writing this paper. While feedback was sought, neither the ADA nor any ADA member has control over publication of this paper or the analysis presented herein.

[2] The Australian Digital Alliance is a is a broad coalition of copyright users and innovators who support copyright laws that strike a balance between providing reasonable incentives for creators, on one hand, and the wider public interest in the advancement of learning, innovation and culture, on the other. The ADA is funded through subscriptions paid by its members, which include universities, libraries, museums and archives, technology companies, and organisations representing people with a print disability. A full list of the ADA's members can be found here: http://digital.org.au/content/members.

[3] Kimberlee Weatherall, *Internet Intermediaries and Copyright: An Australian Agenda for Reform* (2011), Policy Paper prepared for the Australian Digital Alliance (April 2011) (hereafter '2011 Paper'). The paper is available at http://digital.org.au/our-work/publication/internet-intermediaries-and-copyright-australian-agenda-reform.

[4] Attorney-General's Department, *Online Copyright Infringement Discussion Paper* (2014), Proposal 3.

[5] Productivity Commission, *Intellectual Property Arrangements* (Final Report No 78, September 2016), Recommendation 19.1. The Australian government also sought submissions on the question of safe harbour expansion in 2011.

[6] Exposure Draft, Copyright Amendment (Disability and Other Access Measures) Bill 2016 (available at https://www.communications.gov.au/file/13726/download?token=0Fg19Fuv).

involving a high risk of liability for copyright infringement, *orange* indicated the legal situation was unclear, and *green* indicated a low or non-existent risk of copyright infringement (perhaps conditional on the fulfilment of certain conditions, such as taking infringing material down on receiving notice). Table 1 updates the 2011 table, and expands the jurisdictions to include Israel, and other countries in the region with which Australia has comprehensive trade agreements.

Table 1: How risky is the internet intermediary business?

Country	Providing internet access (IAP)	System level/proxy caching	Hosting (Cloud Computing)	Hosting a user-generated site	Running a search engine or similar
Australia: carriage service provider	Green	Green	Green	Green	Green
Australia: other online service provider	Green	Red	Red	Red	Red
Australia – public sector institutions on passage of Bill	*Green*	*Green*	*Green*	*Green*	*Green*
United States	Green	Green	Green	Green	Green
Canada	Green	Green	Green	Green	Green
European Union	Green	Green	Green	Orange	Orange
United Kingdom	Green	Green	Green	Orange	Orange
New Zealand	Green	Green	Green	Orange	Red
Singapore	Green	Green	Green	Green	Green
Japan	Green	Green	Red	Red	Green
South Korea	Green	Green	Orange	Orange	Orange
Israel	Green	Green	Orange	Orange	Orange

Although there is discussion around safe harbours and intermediaries in a number of countries, as discussed in detail below, with some specific proposals to impose some additional obligations on certain kinds of service providers, in particular larger/commercial user-generated content sites, in no country listed in this table is there serious consideration that safe harbours should be repealed. In some countries, additional obligations for commercial user-generated content sites the subject of discussion (in particular in the EU, discussed below, which has raised at the Commission level whether certain user-uploaded content sites should not have the benefit of the hosting safe harbour).

Overall, Australia remains an outlier in:

1. the extent to which it currently imposes copyright liability on internet intermediaries, whether those intermediaries are start-ups, established businesses or public sector institutions;
2. The way that it distinguishes between different kinds of internet intermediaries in imposing copyright risk.

Internet intermediaries in Australia can face copyright liability **regardless whether they cooperate with rights holders or remove infringing material on notification** (notice and take-down), because Australian copyright law holds that a person (or company) that establishes a technical system to reproduce or make works available online will (often) be **directly** liable for copyright infringement (rather than liable for authorising infringements by people who use the system to copy or communicate copyright material). When an entity directly infringes copyright, knowledge of the infringement and even taking precautionary steps to reduce or avoid infringement are irrelevant. Depending on the circumstances and the kind of content involved, this issue is not always readily solved by licensing because so much material is protected by copyright. Licensing everything may be impractical, if not impossible.

Australia is currently proposing to extend safe harbours to educational institutions, cultural institutions and organisations that assist people with disabilities.[7] No other country draws distinctions in this way to exclude most (but not all) private sector entities, including those not making a business out of the dissemination of copyright content – from the protection – and the obligations – of the safe harbours.

This update focuses on cases and legislative changes post-2011. The analysis is based on a review of most recently translated and available copies of legislation and secondary sources. It is not based on practice, including any practice whereby copyright owners might refrain from suing for infringement.[8] This paper does not engage with the rationale for online safe harbours.[9] The interest here is solely in assessing the current state of the law in a range of jurisdictions against which Australia would commonly seek to compare itself. The question is: *is being an internet intermediary riskier, from a copyright perspective, in Australia than in comparable jurisdictions?* The answer is **yes**.

[7] *Copyright Amendment (Service Providers) Bill 2017* (Cth).

[8] There have been a number of studies focused on documenting the practice of US intermediaries operating under the US legal regime: see, eg, Jennifer Urban, Joe Karaganis and Brianna Schofield, *Notice and Takedown in Everyday Practice* (March 22, 2017). UC Berkeley Public Law Research Paper No. 2755628. Available at SSRN: https://ssrn.com/abstract=2755628. See also Daniel Seng, 'The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices' (2014) 18 *Virginia Journal of Law and Technology* 369.

[9] That would require a far more extensive legal, ethical, and economic analysis than has been conducted here. For a recent discussion that teases out the complexities around the safe harbours as they operate in the US, see Matthew Sag, 'Internet Safe Harbours and the Transformation of Copyright Law' (2017) 93 *Notre Dame Law Review*, available at https://ssrn.com/abstract=2830184

Background: internet intermediaries and the safe harbours

An internet intermediary is anyone – in general a company or institution – that provides the basic infrastructure of the Internet, and digital services and platforms. Internet access providers (IAPs), web hosts and cloud providers, and online platforms for the creation and exchange of content (such as YouTube, WordPress, Facebook, Reddit, as well as small blogs, individual websites that allow for any user interaction) are all internet intermediaries. So are many public institutions that provide internet access and host content: including every school, university, and library, and many significant galleries and museums. Internet intermediaries include both local and overseas commercial entities. They are *intermediaries* in the sense that they operate the infrastructure and services that connect end-users with content or other material. They risk infringing copyright when their users infringe.

Their liability arises in a range of very common activities that are essential to the operation of the internet, including:

1. providing internet access;
2. caching/proxy caching;
3. 'traditional' web hosting/cloud hosting;[10]
4. hosting user-generated or user-created content;[11] and
5. operating a search engine.

In undertaking these activities, computers and software operated by internet intermediaries:

- reproduce (temporarily, or for longer periods) and communicate (transmit or make available) copyright material. This (if done without permission or exception) infringes copyright regardless of the knowledge of the intermediary or the steps it takes to reduce copyright infringement.
- facilitate reproduction and communication by others, which could make an intermediary liable for authorising infringement depending on a range of considerations such as their degree of knowledge, control, and the steps they take to reduce the risk of infringement.

'**Safe harbours**' are one mechanism for reducing the risk of legal liability of internet intermediaries while providing protection for copyright owners and mechanisms for copyright owners to have their material removed from online access. In many countries intermediaries are protected from having to pay damages for infringement for certain necessary activities that enable the online environment, provided they take certain specified steps to assist copyright owners: in particular, taking down material when notified of alleged infringement by copyright owners. Injunctive relief – eg requiring the intermediary to block a particular user or website - may remain available.[12]

[10] Cloud computing involves providing customers with access to content and software via Internet access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Commonly known cloud providers would include Dropbox or Google Docs. 'Traditional' hosting refers to companies that, in general, host whole sites or subsites managed by others.

[11] By contrast with 'traditional' hosts, a user-generated webhost has their own site that acts as a central platform for the publication of and access to content created by others (classified here as hosting user-generated content). Examples would include YouTube, Twitter, Facebook, but also universities or schools hosting student-generated content directly uploaded by students, or libraries or galleries that might encourage users to upload photos or other media discussing their own experience.

[12] See eg 17 USC §512(j); ECommerce Directive articles 12(3); 13(2); 14(3); Copyright Act 1968 (Cth) s 116AG(3)-(4) and s 115A (allowing for orders requiring an internet access provider to block certain flagrantly infringing websites).

Safe harbours exist across a range of areas of law.[13] Some safe harbours are found in 'horizontal' rules (such as those found in the EU's Ecommerce Directive[14]) and apply to protect from liability under a range of different laws; others are found in copyright legislation (as in the US,[15] Australia,[16] South Korea[17] and Singapore[18]).

Safe harbours are a place to shelter from a potential storm of liability, but intermediaries can choose to 'risk the high seas' and take other precautions. Safe harbours do not preclude internet intermediaries from taking additional steps to enforce or licence copyright material, although obviously they can affect the incentives of internet intermediaries to do so.[19] In the US major intermediaries which host content have instituted "DMCA plus" measures (the DMCA being the US legislation that enacted copyright safe harbours).[20] "DMCA plus" measures may include pro-active content filtering (preventing material identified in advance by copyright owners from being uploaded) or giving major copyright owners direct access to take infringing material down. Entities that have safe harbours available to them may also (and do) choose to enter licences with significant copyright owners, for example to reduce the number of takedown notices they receive, enable more efficient handling of infringement allegations, or to enable them to do more with copyright content. For example, in Australia, YouTube has a licence agreement with APRA/AMCOS.[21]

Recent Legal Developments in Australia

Australia

Legislation

In Australia, liability for infringing copyright, and authorising infringement, arise under ss 36 and 101 of the *Copyright Act 1968* (Cth). Copyright owners have the exclusive right to **reproduce/copy and communicate** copyright works. Some 'technical' copies are excluded from infringement under ss 43A, 43B, 111A; 111B. But these exceptions are not useful to intermediaries where customers deal with infringing materials, because they are confined to otherwise non-infringing activities.[22]

Safe harbours for the benefit of internet intermediaries, that purport to protect from (direct and secondary) liability for copyright infringement by end-users, are found in Part V Div 2AA of the Act.

---

[13] For a discussion of safe harbours in Australia traversing a range of areas of law, see Peter Leonard, 'Building Safe Harbours in Choppy Waters – Towards a Sensible Approach to Liability of Internet Intermediaries in Australia' (2010) 29 *Communications Law Bulletin* 10.

[14] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* OJ L 178, 17.7.2000, p. 1–16 (hereafter 'Ecommerce Directive'). 'Horizontal' means simply that the protection applies across areas of law, such as defamation, trade mark, copyright, misleading communications, negligent misstatements etc.

[15] US Copyright Act, 17 USC §512.

[16] Copyright Act 1968 (Cth) Part V Div 2AA.

[17] See below page 28.

[18] See below page 24.

[19] For a detailed discussion see Sag, above n 9.

[20] See Urban et al, above n 8.

[21] See http://apraamcos.com.au/10388.aspx.

[22] See generally 2011 Paper, above n 3; see also Australian Law Reform Commission, Report No. 122: *Copyright and the Digital Economy* (2013), Chapter 11. Other provisions (s 39B and 112E) stating that a person who provides facilities for making, or facilitating the making of a communication is not taken to have authorised infringement merely because someone uses the facilities to infringe has been characterised by the High Court as a provision inserted for the avoidance of doubt, and of little practical effect: *Roadshow Films Pty Ltd v iiNet Ltd* [2012] HCA 16; (2012) 248 CLR 42.

But Part V Div 2AA applies only to *carriage service providers* – in essence, providers of telecommunications network infrastructure.[23] Start-ups; other commercial online service providers, schools, universities and other public and cultural institutions cannot rely on the safe harbours. In this respect Australian law remains non-compliant with the Australia-US Free Trade Agreement which requires safe harbours that provide limitations regarding the scope of remedies available against service providers for copyright infringements that they do not control, initiate, or direct.[24] Australia's failure to extend the safe harbours was a legislative error which remains uncorrected over a decade on from AUSFTA.

In 2015 Australian copyright owners were provided with a new tool to address online copyright infringement, s 115A of the *Copyright Act 1968*.[25] Section 115A allows a copyright owner to seek an injunction to require one or more carriage service providers to take reasonable steps to disable access to an online location outside Australia that infringes, or facilitates an infringement of, their copyright and which has the primary purpose of infringing, or facilitating the infringement of, copyright (whether or not in Australia). Section 115A grants a discretion to the court; in exercising that discretion the court is required to take a number of factors into account, including, for example, the flagrancy of the infringement, whether the owner or operator of the online location demonstrates a disregard for copyright generally, and whether such an injunction is a proportionate response. To date the Federal Court of Australia has issued three judgments under s 115A, and made orders blocking a range of overseas sites including The Pirate Bay, Torrenthound, Isohunt,[26] KickAss Torrents,[27] and YesMovies and Project Free TV.[28] Costs are shared between copyright owners and ISPs.

Proposals to couple s115A with an expansion of Australia's safe harbours (and of authorisation liability) were not followed through. At the time that the 2015 amendments were introduced, the Australian government encouraged industry negotiations with a view to introducing a scheme whereby ISPs would pass notices of infringement (and educational materials on copyright) to infringing users identified by copyright owners. Negotiations resulted in a draft code of practice,[29] but did not resolve a number of questions, including the allocation of costs. Discussions were discontinued in early 2016.[30]

In December 2017 the Australian Government introduced the *Copyright Amendment (Service Providers) Bill* 2017. The Bill would extend the definition of 'service providers' to include (in addition to carriage service providers):

---

[23] 'Carriage service providers' are defined in accordance with s 87 of the *Telecomuunications Act 1997* (Cth).

[24] *Australia–US Free Trade Agreement*, signed 18 May 2004, [2005] ATS 1 (entered into force 1 January 2005), art 17.11.29. Under AUSFTA, intermediaries must have policies for the termination of repeat infringers' accounts, and must expeditiously remove infringing materials (subject to a scheme for reinstatement where users can challenge an allegation of infringement). Failure to qualify for the regime, through non-compliance with the conditions, does not necessarily mean that the intermediary is liable: copyright infringement must still be proven.

[25] Introduced by the *Copyright Amendment (Online Infringement) Act 2015* (Cth).

[26] *Roadshow Films Pty Ltd v Telstra Corp Ltd* (2016) 122 IPR 81; [2016] FCA 1503; *Universal Music Australia Pty Ltd v TPG Internet Pty Ltd* [2017] FCA 435 (2017) 348 ALR 493; *Foxtel Management Pty Ltd v TPG Internet Pty Ltd* [2017] FCA 1041 (2017) 349 ALR 154.

[27] *Roadshow Films Pty Ltd v Telstra Corp Ltd* (2016) (2016) 122 IPR 81; [2016] FCA 1503.

[28] *Foxtel Management Pty Ltd v TPG Internet Pty Ltd* [2017] FCA 1041 (2017) 349 ALR 154.

[29] A copy of the draft code is available from the Communications Alliance: http://www.commsalliance.com.au/__data/assets/pdf_file/0005/48551/C653-Copyright-Notice-Scheme-Industry-Code-FINAL.pdf.

[30] Allie Coyne, 'ISPs 'blindsided' by shelved Australian piracy code', ITNews, 18 February 2016, available at https://www.itnews.com.au/news/isps-blindsided-by-shelved-australian-piracy-code-415324.

- an organisation assisting persons with a disability;
- bodies that administer an educational institution;
- certain libraries (the Parliamentary library, and libraries where all or part of the collection comprising the library is accessible to members of the public directly or through interlibrary loans) (for relevant activities); and
- bodies which administer an archive, or a key cultural institution (for relevant activities).

The Bill will improve the legal risk that faces certain key public sector institutions, although the safety appears incomplete. It is not clear on the face of the Bill whether third party service providers undertaking activities *on behalf of* any of these entities (eg, external cloud providers) will have the protection of the safe harbours. This could leave schools, universities, libraries and archives with a legal risk if required in their service contracts to indemnify private sector service providers for copyright infringement. Independent research entities (such as the CSIRO) will not benefit under the Bill. The Bill also leaves Australia non-compliant with the Australia-US Free Trade Agreement, in that there are a large number of entities that provide caching, hosting or other intermediary services which will not have the benefit or the copyright enforcement obligations of the safe harbours. In the second reading speech, the Minister has indicated an intention to further consider the position of other service providers.

Cases

Since 2011 the cases have increased the risk of liability for most internet intermediaries in Australia, with the exception of internet access providers (IAPs), because both direct and authorisation liability have been broadly interpreted by Australian courts.[31]

IAPs are protected as a result of the High Court decision in *Roadshow v iiNet.* The court held that internet access providers (IAPs[32]) are not liable for authorising infringements by their customers engaged in using BitTorrent to download films and television shows.[33] The Australian Federation Against Copyright Theft, acting on behalf of copyright owners, had documented BitTorrent sharing by iiNet customers, and sent notices of infringement to iiNet including this information sufficient to identify subscriber accounts alleged to be involved. AFACT's notices demanded that iiNet prevent the accounts from being used to infringe copyright, and 'take any other action available under iiNet's Customer Relationship Agreement (CRA) which was appropriate having regard to their conduct'. The CRA gave iiNet the right to terminate service for illegal conduct. iiNet took the view that it had no obligation to act.

The High Court held that iiNet was not liable, for two key reasons. First, IAPs, which provided neither the BitTorrent software nor content, only had limited and indirect power to prevent customer infringements via BitTorrent (for example, by terminating access). Second, in the circumstances of that case, issuing warning notices to customers, suspending or terminating their accounts were not

[31] Another proceeding relevant to internet access providers but not to their liability is the application for preliminary discovery brought by Dallas Buyers Club (DBC) against ISP iiNet.[31] DBC sought the names and addresses of iiNet customers who had been 'identified' as infringing copyright the film *Dallas Buyers Club* (in the sense that they were iiNet customers to whose accounts IP addresses involved in the alleged infringements were assigned at the relevant time). The judgment confirms the power of the court to issue an order requiring the provision of contact details, but also confirmed the court's discretion to supervise the use of information obtained via such means and the terms of any communications sent to the ISP's customers. The court was not satisfied with initial draft proposed communications and the proceedings were eventually discontinued without resolving the court's concerns, meaning that the information was not provided by iiNet.

[32] IAPs are commonly called "ISPs" in Australia. This terminology however has potential to be confusing when discussing an international context where "ISP" is often a broader concept comprehending all internet intermediaries. Hence the term IAP is used in this paper.

[33] *Roadshow Films Pty Ltd v iiNet Ltd* [2012] HCA 16; (2012) 248 CLR 42.

reasonable steps.[34] The case thus clarified that '[i]n general, in the absence of any positive steps that actively incite infringement, [IAPs] that provide internet access (as opposed, for example, to hosting services) will not be liable for authorising copyright infringements committed by their subscribers (or those using their accounts)'. As Lindsay notes, this has reduced IAPs' incentive to cooperate in addressing copyright infringement, although IAPs can since 2015 be required to block flagrantly infringing websites.

The impact of *Roadshow v iiNet* on other internet intermediaries was less clear. The judgments in *iiNet* appear to adopt a narrower view of authorisation than prior Australian cases and place greater emphasis on whether the alleged authoriser has granted, or purported to grant, permission to undertake the infringing act. But the High Court's endorsement of the earlier *Moorhouse* decision implies that a person who omits to act, or is indifferent to infringements, may still, in appropriate circumstances, be liable.[35]

The *iiNet* litigation considered the safe harbours at the Full Federal Court level (the High Court did not discuss Part V Div 2AA).[36] iiNet argued that it had a policy for the termination of repeat infringers: it would terminate account holders if they confessed to copyright infringement or had been held liable by a court. The Full Federal Court held that this was *not* a policy for the termination of repeat infringers, as many, or even most repeat infringers would not have their accounts terminated. This is worth noting, because it suggests Australian courts are prepared to judge the adequacy of internal policies of service providers under the safe harbours. This should give copyright owners some assurance that beneficiaries of the safe harbours will be required genuinely to cooperate in copyright enforcement.

The **direct** liability of other service providers engaged in commercial activity involving copying and communication of content online was potentially expanded in the decision of the Full Federal Court in the *Optus TVNow* case.[37] Telecommunications company Optus had created a cloud-based system to enable its mobile internet customers to record and then watch free-to-air television using software developed and maintained by Optus, and on Optus' servers). The court held that by designing and operating an automated copying system configured specifically to respond to a user's command to make a copy, Optus was a **joint maker** of any resulting copies along with the consumer who actually 'pressed the record button'.[38] Although the Full Federal Court was careful to state that its findings might not be generalizable to other cloud computing services, the decision undoubtedly increased the risk of liability for any operator of cloud services (which, of their nature, involve the establishment of automated systems for making copies of content at the instance of a user/customer) and every other internet intermediary, which of necessity establish systems designed to copy and communicate material.[39]

Further clarity regarding the potential liability of internet intermediaries engaged in hosting content has recently been provided in *Pokémon Company International, Inc v Redbubble Ltd* [2017] FCA 1541. The case involved a complaint against internet company Redbubble by the Pokémon company, owners of copyright in a range of characters, including a bright yellow character known as Pikachu. Redbubble's technology allows artists and designers to upload images and designs for use on

[34] David Lindsay, 'ISP Liability for End User Infringements: The High Court decision in *Roadshow Films v iiNet*' (2012) 62(4) *Telecommunications Journal of Australia* 53.1.
[35] Ibid, 53.19-53.21.
[36] *Roadshow Films Pty Ltd v iiNet Ltd* (2011) 89 IPR 1.
[37] *National Rugby League Investments Pty Ltd v Singtel Optus Pty Ltd* (2012) 201 FCR 147; [2012] FCAFC 59
[38] *National Rugby League Investments Pty Ltd v Singtel Optus Pty Ltd* (2012) 201 FCR 147; [2012] FCAFC 59, [64]-[77].
[39] See the discussion in Rebecca Giblin, 'Stranded in the Technological Dark Ages: Implications of the Full Federal Court's Decision in NRL v. Optus' (2012) 35 *European Intellectual Property Review* 632-641.

products like T-shirts. Customers order products through the Redbubble website (operated on servers not based in Australia, although the company is listed on the Australian Stock Exchange). Products are manufactured and dispatched by third party companies (fulfillers). These processes were automated. At the time of the conduct giving rise to the case, Redbubble had taken a range of precautions against the risk of copyright infringement, including requiring artists to agree that they owned or had permission to use copyright in uploaded works, establishing processes for copyright owners to notify potential infringements, and blocking certain keywords as search terms. But Redbubble sought to avoid preventing allowable parodies and non-infringing activity, and hence did not prohibit trade marks as keywords in a blanket way.

The court held that Redbubble had infringed in three separate ways, both directly and by authorising copyright infringement.

Redbubble directly infringed copyright by communicating infringing works (the artistic images) to the public in Australia. Uploading artists originated the infringing images, but Redbubble still determined the content of communications to customers 'through its processes, protocols and arrangements with the artists'.[40] The fact that Redbubble 'has a user agreement with artists which deals with matters including the possibility of infringing materials, an IP policy, and a team dedicated to deal with impermissible content' was cited by the Trial Judge as *supporting* Redbubble's responsibility for communicating the images to the public.[41] This creates perverse incentives: it means that taking steps to address copyright enforcement leads to responsibility and potential liability. This is the kind of result that safe harbours seek to avoid.

Redbubble also knowingly exhibited infringing articles in public by way of trade.[42] Although not the manufacturer of infringing articles, Redbubble 'exhibited articles in public by projecting images on products which were able to be sold to potential customers'.[43] Once Redbubble had specific knowledge (provided by letter from the copyright owner) of characters alleged to be infringed, it had the actual or constructive knowledge required for liability.[44]

Finally, Redbubble authorised the reproduction of copyright material through manufacture and sale of infringing articles by third party fulfillers in Australia. Redbubble had a commercial relationship with the fulfillers (and received a percentage of the product price). It also had some power to prevent the infringements, since although its systems were automated, it designed and operated the system, and had 'absolute power' to alter it.[45] In terms of the reasonable steps Redbubble had taken to reduce or prevent infringement, Redbubble had a public IP policy, and content team that monitored the accounts of artists who had material taken down, with potential actions including sending a warning, restricting, suspending or deleting the account (or continuing to monitor the account). Redbubble could have blocked the upload of content tagged with trade mark terms (like Pikachu), but had taken the view that while easier and cheaper, such a system would prevent artists using words in legitimate non-infringing ways. Redbubble did promptly remove infringements that were identified to it.[46] The court noted both that there were other reasonable steps Redbubble

[40] *Pokémon Company International, Inc v Redbubble Ltd* [2017] FCA 1541 [48].
[41] Ibid.
[42] Contrary to *Copyright Act 1968* (Cth) s 38.
[43] *Pokémon Company International, Inc v Redbubble Ltd* [2017] FCA 1541 [52].
[44] The judgment does not state whether the notification by the copyright owner in November 2015 specifically identified URLs for products alleged to be infringing, stating only that the correspondence ""in all Pokémon characters, including 30 characters" that were specifically identified. That letter identified conduct which was claimed, amongst other things, to be the sale or offering for sale of infringing images on Redbubble products within the meaning of s 38 of the Copyright Act": *Pokémon Company International, Inc v Redbubble Ltd* [2017] FCA 1541 [54].
[45] *Pokémon Company International, Inc v Redbubble Ltd* [2017] FCA 1541 [58].
[46] *Pokémon Company International, Inc v Redbubble Ltd* [2017] FCA 1541 [66].

could have taken, and that it had taken many reasonable steps to prevent infringement.[47] The court concluded:

> *The business established by Redbubble carried the inherent risk of infringement of copyright of the kind complained of by TPCi. It is true that Redbubble sought to mitigate the risk, but it was an inevitable incident of the business, as Redbubble chose to conduct it, that there were likely to be infringements. It could have prevented them by taking other steps but for business reasons Redbubble chose to deal with the risk of infringement by a process that enabled the infringements to occur. Such infringements were embedded in the system which was created for, and adopted by, Redbubble. There may have been a sound commercial basis for Redbubble to manage the risks of infringement as it did, but in doing so it authorised the infringements which occurred.*[48]

Prompt *ex post* removal of notified copyright infringement was insufficient – at least on the circumstances of *this* case – to avoid authorisation liability. This is striking: it suggests that, in Australia, companies that engage in a business that risks some copyright infringement (which arguably is most companies that enable user interaction online) can be liable for authorising infringement if they fail to prevent that infringement, *despite taking extensive and reasonable steps to mitigate that risk*. In the view of the trial judge, Redbubble was required to take steps that would significantly increase 'false positives' (blocking legitimate uses of copyright or trade mark content).[49] It should be noted that the court was talking about steps Redbubble could be required to take to avoid the particular infringements involved in the case (*i.e.* those involving Pokémon characters). Effectively, the court appears to be demanding 'takedown and stay down' – specific actions to ensure that infringements do not reappear. The court did not appear to say that Redbubble was obliged *generally* to block tags involving trade mark terms, but to block specific terms once notified that (alleged) infringements were occurring (in the case, some correspondence had been received from the copyright owner in previous years).

This is reinforced by the remedies imposed. The trial judge *refused* an injunction, on the basis that Redbubble had since amended its program (to block content tagged with the trade mark terms), hence there was no risk of continuing infringement. The court also ordered only nominal damages of only AU$1, because no harm was proven: the relevant products were not such as would have been sold by the Pokémon company itself. No additional damages were available because Redbubble had not acted in flagrant disregard of the copyright owner's rights. It is not clear what the result would have been had different evidence been offered on the nature of the harm.

An appeal was filed in the Redbubble case on 5 February 2018.

The result in *Pokémon Company International, Inc v Redbubble Ltd* [2017] FCA 1541 is not 'responsibility without liability', like the website blocking system or developments in Europe.[50] Redbubble may not have been entitled to rely on the safe harbours, at least in relation to its potential liability for authorising physical infringements in the form of products. But it has implications for all online intermediaries. If the result is upheld on appeal, internet intermediaries

---

[47] *Pokémon Company International, Inc v Redbubble Ltd* [2017] FCA 1541 [61]-[62].

[48] *Pokémon Company International, Inc v Redbubble Ltd* [2017] FCA 1541 [67].

[49] Redbubble argued in the case that many of the images identified as infringing were in fact parodies and hence protected by s 41A of the *Copyright Act*. This argument was rejected by the court, which concluded that there was no evidence of the intention (parodic or otherwise) of the creator of the images, and in on their face, the images were attempts to 'cash in' on the fame of the images, rather than to engage in parody (even where the images were amusing).

[50] Graeme Dinwoodie, 'A Comparative Analysis of the Secondary Liability of Online Service Providers', in Graeme Dinwoodie (ed), *Secondary Liability of Internet Service Providers* (Springer, 2017), 1, 3.

who fail to do everything possible to prevent infringement (even steps that will have significant impact on non-infringing activity) can face liability and an injunction, and possibly damages if harm can be proven – for example if there was evidence that some products competed with products of the copyright owner. And even an intermediary who takes all possible actions to mitigate the risk of infringement is still **directly** infringing when infringements occur. It remains to be seen how far such reasoning extends beyond 'businesses carrying the inherent risk of infringement' to, say, non-profit intermediaries hosting user-generated materials, or schools hosting student materials and interactions.[51] On the other hand, the decision has been characterized as a pyrrhic victory given the absence of monetary remedies.

Summary

The **upshot** in Australia is that:

- IAPs merely providing internet access are unlikely to be held liable for the infringements of their subscribers even if they take no action to notify or educate infringing customers. But they can be required to block overseas sites that flagrantly infringe copyright.
- On the other hand, *other* online intermediaries face a significantly higher risk of infringement than in 2011. Schools, universities, libraries, galleries, web hosts, cloud computing platforms and other analogous online service providers, platforms supporting user-generated content, and search engines:
    - face a serious risk of **direct** infringement through communication or reproduction initiated by their users;
    - can in some circumstances be held liable for exhibiting infringing articles by way of trade once fixed with knowledge of infringement; and
    - If the judgment in *Pokémon Company International, Inc v Redbubble Ltd* [2017] FCA 1541, also face a high risk of liability for **authorising** infringement despite taking extensive steps to mitigate the risk of infringement.
- There has been no reform to exceptions or the safe harbours which might ameliorate that risk.

Recent Developments in Intermediary Liability outside Australia

United States

Legislation

In the United States, the relevant legislation is the *US Copyright Act* 1976. Direct liability for copyright infringement arises under §501 of the Act, and two forms of secondary liability (contributory and vicarious liability) are well-established in the case law. In 1998 the *Digital Millennium Copyright Act* (DMCA) amended the 1976 Act to include §512, which provides safe harbours that offer protection for online service providers from direct and secondary liability for copyright infringement by end-users, subject to the fulfilment of certain conditions,[52] including a notice-and-takedown regime whereby copyright owners can get infringing materials removed from

[51] As Dinwoodie notes, 'the legitimacy of the behaviour of intermediaries occupies a spectrum that requires greater flexibility (and room for more subtle calibration) than formal secondary liability doctrine might seem to allow. Indeed, such flexibility is necessary also to account for the different demands that might be imposed on smaller entities without he capital or sophistication of [the larger players]': ibid, 25.

[52] The On-Line Copyright Infringement Liability Limitation Act (OCILLA), commonly known as Section 512 of the DMCA, is codified as Title II of the DMCA at 17 U.S.C. § 512 (2012).

online sites without having to bring a lawsuit by sending notices to OSPs to have material removed from hosted sites or search engine indexes. §512 is the model for the provisions in AUSFTA.

The legislation for the DMCA safe harbours has not been amended since 1998,[53] despite significant developments in technology since that time (Google, Facebook, peer-to-peer file-sharing, YouTube and other user-generated content sites all post-date the development of the DMCA provisions, and arguably owe some part of their existence and growth to those safe harbours).

There were proposals for additional enforcement mechanisms in 2012 (these would not have affected the safe harbours). The *Stop Online Piracy Act,* or *SOPA*, was proposal put to US Congress to enable the enforcement of copyright and trade mark law against foreign 'rogue' websites. *SOPA* would have enlisted a range of new intermediaries in online enforcement: in particular, domain name servers, credit card providers and online advertising service providers (as well as imposing additional obligations on search engines). *SOPA* became controversial, especially for its proposed intervention in the fundamental systems that link domain names to IP addresses. It was withdrawn from 2012 after significant on- and offline protest.[54]

In recent times, §512 has been the subject of significant debate and discussion – but no concrete proposals for reform. In April 2013, the Chairman of the House Committee on the Judiciary Bob Goodlatte announced that a comprehensive bipartisan review would be conducted into Copyright law in the United States to assess the laws efficacy in the digital age. A number of hearings were conducted by the Committee in the period between March 2013 and April 2015. In December 2016, the committee published its first policy proposal document (which did **not** address safe harbours)[55] and called for public comments by January 2017.[56] No further developments are noted on the Committee's website. The focus of the House Judiciary Committee on matters other than safe harbour reform is important, as it represents Congress' current priorities.

There have been other discussions outside Congress. In July 2013, the US Department of Commerce's Internet Policy Task Force, led by the US Patent and Trademark Office (USPTO) and National Telecommunications and Information Administration (NTIA), issued a green paper on Copyright Policy, *Creativity and Innovation in the Digital Economy*,[57] which, among other things, called for a multi-stakeholder dialogue on how to improve the operation of the safe harbours' notice and takedown system. The Task Force subsequently held a number of roundtables, public meetings and forums on these questions, most recently in January 2018. The United States Copyright Office is also in the midst of a public study to evaluate the impact and effectiveness of the safe harbour provisions.[58] The Copyright Office in the United States is at present reviewing submissions, empirical evidence submitted, and transcripts following a public consultation. This process began in December 2015 with a notice of inquiry and two round tables in May 2016. The public inquiry has received tens

[53] As noted above, a broadening of the safe harbours to cover all online service providers was proposed in the *Online Copyright Infringement Discussion Paper* (2014), and in an exposure draft of the Copyright Amendment (Disability Access and other Measures) Bill 2016: see above nn 4-6. The Productivity Commission also recommended extension of the safe harbour in its final report on Australia's IP Arrangements: above n 5.

[54] For a discussion, see Kimberlee Weatherall, 'Evaluating SOPA: Who Should Enforce IP Online?' (2012) 62(4) *Telecommunication Journal of Australia* 59.1-59.13.

[55] See https://judiciary.house.gov/wp-content/uploads/2016/12/Copyright-Reform.pdf

[56] These can be accessed at https://judiciary.house.gov/issue/us-copyright-law-review/#section-5.

[57] The Green Paper is available at https://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf.

[58] See https://www.copyright.gov/policy/section512/.

of thousands of submissions.[59] As at 1 February 2018, no results from the inquiry are presently available. It is not clear when further developments in these external inquiries can be expected.

There have also been a number of independent studies of the US notice-and-takedown system, including a paper by Seng[60] and a large empirical study of online service provider practice and takedown notices conducted by Urgan, Karaganis and Schofield.[61] The latter study concluded that:

1. The DMCA safe harbours are deeply embedded in the practice and policies of both online service providers (OSPs) and copyright owners. Their liability protections remain central to OSPs' sense of their freedom to operate, and fundamental to their survival in a context where high statutory penalties for infringement could easily sink companies. Copyright owners agreed that notice and takedown is fundamental to their enforcement strategies, but uniformly described its provisions as inadequate for addressing large-scale online infringement.[62]
2. There is significant variation in practice. While some copyright owners, and some online service providers engaged in large-scale, automated infringement detection and removal (in some cases going beyond the requirements of the DMCA, voluntarily using technological means to further block the distribution of infringing materials before they become available online), other OSPs receive small numbers of notices and review them manually.

Given these findings, it seems unlikely that the outcome of the present discussions in the Copyright Office and beyond around the operation of the DMCA safe harbours will be a wholesale reconsideration of the approach found in §512, although next steps remain unclear.

A final point of note is that the US' Copyright Alert System, a memorandum of understanding whereby IAPs passed on notices of infringement to their subscribers, with potential for escalating penalties, and which commenced in 2013, was terminated in 2017.[63]

Case law

There have been a number of cases considering the US safe harbours since 2011. They have clarified certain aspects of the safe harbours without, however, changing their architecture, and without fundamentally changing the parties who can rely on them.

There have been a number of decisions considering when an internet intermediary will have sufficient knowledge of an infringement that it is obliged to act on that knowledge (ie remove

[59] A total of 92,398 submissions are available online. In November 2016, the Copyright Office sought further comment in the form of opinions and empirical studies specifically addressing the impact and effectiveness of the DMCA safe harbor provisions, and there are 79 Additional Comments available on regulations.gov. There are also 9 empirical studies are available on regulations.gov.

[60] Daniel Seng, 'The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices' (2014) 18 *Virginia Journal of Law and Technology* 369.

[61] Jennifer Urban, Joe Karaganis and Brianna Schofield, *Notice and Takedown in Everyday Practice* (March 2017).

[62] See similarly Maayan Perel and Niva Elkin-Koren, 'Accountability in Algorithmic Copyright Enforcement' (2016) 19 *Stanford Journal of Law and Technology* 473, 473 ('the Notice and Takedown (N&TD) regime has become ubiquitous and embedded in the system design of all major intermediaries: major copyright owners increasingly exploit robots to send immense volumes of takedown requests and major online intermediaries, in response, use algorithms to filter, block, and disable access to allegedly infringing content automatically, with little or no human intervention').

[63] Ted Johnson, 'Internet Service Providers, Studios and Record Labels Call it Quits on Copyright Alert System', *Variety*, 27 January 2017, available at http://variety.com/2017/digital/news/copyright-alerts-piracy-mpaa-comcast-att-1201971756/.

infringing material) or risk losing any entitlement to rely on the safe harbour.[64] 'Red flag' knowledge arises when a service provider is 'aware of facts that would have made the **specific** infringement 'objectively' obvious to a reasonable person'; 'The infringement must be immediately apparent to a non-expert.'[65] *Generalised* knowledge that infringement is occurring is insufficient to deprive an intermediary of the safe harbours.

This issue was considered in *Capitol Records, LLC v. Vimeo*,[66] in which copyright holders of various sound recordings and compositions sued Vimeo, a user-uploaded video content hosting website. The rights holders alleged that Vimeo was responsible for the copyright infringement in the audio content of 200 videos on the website and had evidence that Vimeo employees had viewed videos containing the copyright material. The Second Circuit held that this in itself was not sufficient to create knowledge that would disentitle Vimeo from relying on the safe harbours: the question was whether infringement was obvious to a person without specialised understanding of music or copyright law. In proving disentitlement to DMCA protection, a plaintiff needs to identify specific instances where red flag knowledge or wilful blindness has occurred and cannot rely on generalisations.[67] The court also emphasised that voluntary monitoring of videos visual content did not deprive it of DMCA protection in relation to audio content.

Similar issues were considered in *Viacom International v YouTube, Inc* 676 F.3d 19, 34 (2nd Cir 2012). In that case Viacom alleged direct and secondary copyright infringement based on 79,000 audiovisual clips that appeared on YouTube between 2005 and 2008. Viacom complained that YouTube was aware of very widespread infringement and was therefore liable unless it acted to take material down. The 2nd Circuit held that wilful blindness can disqualify a service provider, but the provider must be turning a blind eye to *specific and identifiable* instances of infringement, not failing to make inquiries in the face of general awareness that some activity is infringing.[68]

There has also been some discussion in the cases around when a web host will be so involved in the activities of users that it is no longer merely hosting material 'at the direction of the user'.[69]

Another important case is *BMG Rights Management LLC v Cox Communications Inc*,[70] decided by the 4th Circuit Court of Appeals on 2 February 2018. In this case copyright owner BMG sued internet

---

[64] See eg *Mavrix Photographs, LLC v. LiveJournal, Inc.* (2017) 853 F.3d 1020. A photographer sued for infringement of their photographs uploaded to a LiveJournal site. Volunteer moderators led by a LiveJournal employee had reviewed and approved the posting. The matter was remitted for trial. See also *EMI Christian Music Group, Incorporated v. MP3tunes, LLC* , LLC. 844 F.3d 79, a case in which the alleged infringer was held to have actual knowledge of infringements. In that case the websites mp3tunes.com and sideload.com allowed users to store music found online in virtual lockers and search an index of free music to add to the MP3tunes website respectively.

[65] These phrases are interpretations of the statutory text, which states that the service provider cannot rely on the safe harbour if they fail to act where "aware of facts or circumstances from which infringing activity is apparent": §512(c)(1)(A). In *Mavrix Photographs, LLC v. LiveJournal, Inc.* (2017) 853 F.3d 1020 for example, photographs uploaded to the site had watermarks, which might have made infringement obvious (the matter was remitted for trial).

[66] *Capitol Records, LLC v. Vimeo*, LLC 826 F.3d 78 (2d Cir. 2016).

[67] A similar conclusion was also emphasised in *Viacom Intern. Inc. v. YouTube, Inc.* 940 F.Supp.2d 110 (2d Cir 2013).

[68] *Viacom International v YouTube, Inc* 676 F.3d 19, 34 (2nd Cir 2012).

[69] see eg *Mavrix Photographs, LLC v. LiveJournal, Inc.* (2017) 853 F.3d 1020 (see above n 64). In that case there was a live question whether the moderators were agents of LiveJournal, hence involving LiveJournal directly in the infringements. But cf *BWP Media USA, Inc. v. Clarity Digital Group, LLC* 820 F.3d 1175, where the business model of the website was structured such that rather than a centralized writing staff, independent contractors referred to as examiners were the source of content on the website. The Court held that this arrangement did not make the examiners 'agents' and did not preclude reliance on the hosting safe harbour when these independent contractors had uploaded an infringing photograph to the site.

access provider Cox Communications, alleging vicarious and contributory liability for its users' infringing BitTorrent use: in other words, the facts resembled those in *Roadshow v iiNet.* It was held that Cox was unable to rely on the DMCA safe harbour because it did not have or reasonably implement a repeat infringer policy. Although Cox did have a policy for addressing infringing use by subscribers, 'Cox failed to qualify for the DMCA safe harbor because it failed to implement its policy in any consistent or meaningful way — leaving it essentially with no policy'.[71] The jury at first instance had held Cox liable for contributory infringement, but this finding was overturned and remitted to the lower court because the jury at first instance was incorrectly instructed on the level of knowledge required. The 4th Circuit held that for Cox to be liable, BMG would have to show that Cox knew of specific instances of infringement or was willfully blind *i.e.* that it consciously avoided learning about specific instances of infringement). It would not be sufficient that Cox ought to have known of particular infringements or that it knew generally that infringement was occurring.

Another issue is when copyright owners may send a takedown notice. In *Lenz v Universal Music Corp* the 9th Circuit held that a copyright owner was not entitled to send a notice and assert a 'good faith belief that use of the material in the manner complained of is not authorised … by law' where it failed to consider whether the use is a fair use.[72]

Summary

A review of developments in the US suggests that there has been much discussion and review of the DMCA safe harbours. They are however demonstrably woven into the practices of both copyright owners and intermediaries, and they have not prevented some (especially the large) service providers from engaging in much more active enforcement (DMCA-plus). There are, at the time of writing, no current specific proposals for reform with serious political support. The courts have not endorsed attempts to impose obligations to act on generalized knowledge of infringement, but have required service providers to take seriously their obligation to take down material once notified, and to terminate the accounts of repeat infringers. Unlike the Australian court that decided the *Redbubble* case, the US Courts have been solicitous to protect exceptions to copyright infringement.

Canada

Legislation

At the time of the 2011 Paper, there was a Bill before the Canadian Parliament proposing numerous amendments to Canadian law including amendments addressing questions of intermediary liability. These amendments became part of Canadian law in 2012.

---

[70] *BMG Rights Management LLC v Cox Communications Inc* (4th Cir., February 2, 2018).

[71] Cox had a thirteen-strike system. The first notice produced no action. The second through seventh notices resulted in warning emails to the subscriber. After the eighth and ninth notices, Cox would display a warning page, but the subscriber could reactivate their service by clicking an acknowledgement. After the tenth and eleventh notices, Cox suspended services, requiring the subscriber to call a technician, who, after explaining the reason for suspension and advising removal of infringing content, reactivated service. After the twelfth notice, the subscriber was suspended and directed to a specialized technician, who, after another warning to cease infringing conduct, reactivated service. After the thirteenth notice, the subscriber was again suspended, and considered for termination. Cox would accept only one notice per subscriber per day, and reset the thirteen strike 'clock' every 6 months. Cox however always reactivated customers whose accounts were terminated, and then later ceased terminating repeat infringers.

[72] *Lenz v Universal Music Corp* 801 F.3d 1126 (9th Cir. 2015).

Copyright risk arising from providing network access is governed by subsection 31.1(1) of the *Copyright Act 1985,* which provides:[73]

> *A person who, in providing services related to the operation of the Internet or another digital network, provides any means for the telecommunication or the reproduction of a work or other subject-matter through the Internet or that other network does not, solely by reason of providing those means, infringe copyright in that work or other subject-matter.*

This is notably broader than the roughly equivalent ss 39B and 112E of the Australian *Copyright Act 1968* (Cth). Those provisions provide only that a '[a] person (including a carrier or carriage service provider) who provides facilities for making, or facilitating the making of, a communication is not taken to have *authorised* any infringement of copyright in a work merely because another person uses the facilities so provided to [infringe]' (emphasis added). Thus unlike the Canadian provision, the Australian provisions leave open the possibility of direct liability.

Caching is dealt with under subsection 31.1(2), which states that caching works to improve efficiency of telecommunications does not create liability for infringement on part of an intermediary. This protection is contingent upon the intermediary fulfilling certain basic conditions.[74]

Hosting is addressed under subsection 31.1(4), which states that intermediaries who provide hosting of content do not infringe copyright, unless the intermediary knows that there is a 'a decision of a court of competent jurisdiction' which indicates that the entity storing the content infringes copyright in the way they are using that content.

The Canadian Act also exempts search engines from liability for reproduction and communication provided certain conditions are met, including that the search engine must cease their reproduction/communication within 30 days of receiving notice.[75]

The Canadian legislation precludes deliberately infringing intermediaries from taking advantage of these defences: none apply if an intermediary 'provide[s] a service primarily for the purpose of enabling acts of copyright infringement if an actual infringement of copyright occurs by means of the Internet or another digital network as a result of the use of that service'.[76]

In addition *and separately from* these defences, Canada operates a 'notice-and-notice' regime for internet intermediaries (IAPs and hosts) which came into force on 13 August 2014.[77] A copyright owner can report an infringement by sending a notice in writing to an intermediary to which the relevant IP address is assigned. The notice must include the claimant's name, address and interest in copyright, details of the alleged infringement (type, time, location). The intermediary must promptly forward the notice to the accused subscriber, and maintain a record of the user (for a fixed period). The Canadian intermediary is not required to take down material absent a court order. Where the intermediary fails to carry out its obligations, it will be liable for statutory damages ranging from $5,000 to $10,000. The notice and notice regime does not apply to "information location tools" that

[73] Section 31.1(1) is essentially a codification of the existing case law reviewed in the 2011 Paper ie *Society of Composers, Authors, and Music Publishers of Canada v Canadian Association of Internet Providers* [2004] 2 SCR 427

[74] Copyright Act 1985 (Canada)s 31.1(2). The conditions are that the intermediary must not modify the communication (other than for technical reasons); must ensure that technical directions (eg, no-caching directions) specified in accordance with industry practice are executed; and must not interfere with the use of technology that is lawful and consistent with industry practice in order to obtain data on the use of the work or other subject-matter.

[75] Copyright Act 1985 (Canada) s 41.27.

[76] Copyright Act 1985 (Canada) s 27(2.3), 31.1(6).

[77] Copyright Act 1985 (Canada) s 41.25.

are content neutral and not enabling infringement (in which case remedies against them are limited to injunctions).[78]

European Union and United Kingdom

Legislation

European-level and UK-level legislation reviewed in the 2011 Paper has not been amended, but has been extensively interpreted by the courts.[79] The *Copyright in the Information Society Directive*[80] provides relevant copyright exceptions (in particular for the kinds of temporary and technical copies necessary in transmission and caching of copyright material), and the *Ecommerce Directive*[81] provides horizontal safe harbours. Articles 12 to 14 of the *Ecommerce Directive* provide that internet intermediaries are not liable for the content that they transmit, store or host, as long as they act in strictly a passive manner. Articles 12 to 14 of the *Ecommerce Directive* provide that internet intermediaries are not liable for the content that they transmit, store or host, as long as they act in a strictly passive manner. As stated in Recital 42:

> *The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.*

Although there is no specific safe harbour for search engines, the Court of Justice of the European Union has interpreted the hosting provision as applying to search engines where the relevant conditions are met.[82] On obtaining knowledge of the unlawful nature of relevant content, intermediaries must act expeditiously to remove or disable access. Article 15 prohibits Member States from imposing on intermediaries a general obligation to monitor the information transmitted or stored. The safe harbours are subject to the courts' power to issue an injunction requiring an intermediary to act to end infringement even in the absence of liability (discussed below).[83]

---

[78] Copyright Act 1985 (Canada) s 41.27.

[79] There have been amendments to UK copyright legislation in the form of new exceptions for quotation, parody, caricature and pastiche, libraries, education, disabled people, research (text and data mining) and public bodies, which came into force in 2014. These exceptions are not relevant to the technical issues dealt with this paper.

[80] *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society*, O.J. L 167, 22/06/2001 P. 0010 – 0019 ('Information Society Directive'), art 5.

[81] Implemented in the UK via the *Electronic Commerce (EC Directive) Regulations 2002* (SI 2002 No 2013).

[82] Joined Cases C-236/08-C0238/08, *Google France SARL v Louis Vuitton Malletier SA*, 2010 E.C.R. I-2417, ¶¶109-114. This is subject to the requirement that the activities of the search engine are considered to be 'of a mere technical, automatic and passive nature', implying that the service provider 'has neither knowledge of nor control over the information which is transmitted or stored.' Whether in fact a search engine (or indeed any other kind of provider) can rely on the safe harbours depends on the facts of the case and in particular whether the intermediary is operating in a neutral manner – but the detailed application of these standards has, so far, been left to national courts and not finally settled by the CJEU: Dinwoodie above n 51, 36-37.

[83] Information Society Directive above n 80 art 8(3); ECommerce Directive above n 14 art 11.

For internet access providers, the *Copyright in the Information Society Directive* provides exceptions for temporary reproductions occurring in the course of communication, regardless of whether the communication is an infringing one (*Information Society Directive*, Article 5), and establishes, through the *Ecommerce Directive*[84] a safe harbour for 'mere conduits' that has less conditions than the Australian safe harbour (Art. 12): IAPs are not required to have a policy for the termination of repeat infringers. It may be worth noting too that provisions of the UK's *Digital Economy Act 2010* designed to implement a system for sending infringement notices to ISP subscribers was not brought into effect and has been repealed.[85] In 2015 a joint initiative of representatives of the UK's creative industries and major Internet Service Providers (ISPs) was launched, *Creative Content UK,* comprising an education campaign and voluntary system for passing on notices of infringement to subscribers. Website blocking has been implemented via s 97A of the *Copyright, Designs and Patents Act 1988* (UK) and applied in a series of cases (see below).

In relation to caching, all internet intermediaries have the benefit of Article 13 of the *Ecommerce Directive*, which exempts an internet intermediary from any damages award provided that it does not modify the information, complies with any access conditions at the source, and with updating rules communicated in a standard way, does not interfere with technology used to ensure accurate usage data, and removes infringing material on receiving notice of its removal from the source location.

In relation to hosting, a safe harbour applies provided that the host acts expeditiously to remove infringing material on receiving actual or constructive knowledge of an infringement.[86] If the safe harbour applies, the possibility remains that a court will order an injunction to prevent infringement.[87] The EU safe harbour conditions are reasonably similar to those in the US, although again the EU does not require a policy for the termination of the accounts of repeat infringers, and European-level legislation does not set out a detailed system for notice and takedown of material (or for its reinstatement should takedown be unjustified).[88] In a number of areas, best practice guidelines have been developed by IP owners and intermediaries to address infringement. [89]

The safe harbours are the subject of discussion in Europe. In 2015, the Commission set out a strategy for the digital single market (DSM), *inter alia,* indicating an intention to consider the position of online platforms. The Commission expressed some concern that 'some platforms can control access to online markets and can exercise significant influence over how various players in the market are remunerated'[90] and, in that connection, asserted that:

> The principle, enshrined in the e-Commerce Directive, that internet intermediary service providers should not be liable for the content that they transmit, store or host, as long as they act in a strictly passive manner has underpinned the development of the Internet in Europe …

[84] ECommerce Directive above n 14.
[85] Dinwoodie above n 51, 48. The Atc was repealed by the *Deregulation Act 2015* (UK) in light of the success of s 97A of the *Copyright Act.*
[86] ECommerce Directive above n 14 article 14.
[87] *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society*, O.J. L 167 , 22/06/2001 P. 0010 – 0019 (hereafter EU Information Society Directive), Article 8(3).
[88] The Safe Harbour does not apply if the customer is 'is acting under the provider's authority or control'. This is unlikely in traditional web hosting or cloud service provision: *Ecommerce Directive*, above n 14 Article 14.3.
[89] Dinwoodie above n 51, 40-41.
[90] European Commission, 'A Digital Single Market Strategy for Europe' (Communication) COM (2015) 192 final, at 11.

> [Nevertheless, r]ecent events have added to the public debate on whether to enhance the overall level of protection from illegal material on the Internet. In tandem with its assessment of online platforms, the Commission will analyse the need for new measures to tackle illegal content on the Internet, with due regard to their impact on the fundamental right to freedom of expression and information, such as rigorous procedures for removing illegal content while avoiding the take down of legal content, and whether to require intermediaries to exercise greater responsibility and due diligence in the way they manage their networks and systems – a duty of care.[91]

In 2016 the Commission issued a communication on Online Platforms and the Digital Single Market.[92] This communication noted that '[w]hile certain concerns were raised on liability issues the consultation showed broad support for the existing principles of the e-Commerce Directive.'[93] The Commission therefore indicated its intention to 'maintain a balanced and predictable liability regime for online platforms', subject to dealing with certain specific issues – including copyright.

Specifically, the Commission is concerned about the allocation of revenues for the use of copyright-protected content, and whether value generated by new forms of online content distribution that make copyright-protected content uploaded by end-users widely available is fairly shared between distributors and rights holders. This has become known as the issue of the 'value gap'. The Commission indicated an intention to introduce copyright-specific regulations on this point, further address enforcement in relation to counterfeit goods, and engage with platforms regarding voluntary cooperation mechanisms aimed at depriving infringers of revenue from their illegal activities, in line with a 'follow the money' approach.[94]

In September 2016 the Commission issued a Proposal for a Directive on Copyright in the Digital Single Market.[95] The proposal included Article 13 as follows (note that this proposal has since been significantly amended):

> *Use of protected content by information society service providers storing and giving access to large amounts of works and other subject-matter uploaded by their users.*
>
> 1. Information society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users shall, in cooperation with rightholders, take measures to ensure the functioning of agreements concluded with rightholders for the use of their works or other subject-matter or to prevent the availability on their services of works or other subject-matter identified by rightholders through the cooperation with the service providers. Those measures, such as the use of effective content recognition technologies, shall be appropriate and proportionate. The service providers shall provide rightholders with adequate information on the functioning and the deployment of the measures, as well as, when relevant, adequate reporting on the recognition and use of the works and other subject-matter.

[91] Ibid.
[92] European Commission, 'Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe' (Communication) COM (2016) 288 Final.
[93] Ibid, 8.
[94] Ibid.
[95] European Commission, Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market, COM(2016) 593 final, available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17200.

2. Member States shall ensure that the service providers referred to in paragraph 1 put in place complaints and redress mechanisms that are available to users in case of disputes over the application of the measures referred to in paragraph 1.

3. Member States shall facilitate, where appropriate, the cooperation between the information society service providers and rightholders through stakeholder dialogues to define best practices, such as appropriate and proportionate content recognition technologies, taking into account, among others, the nature of the services, the availability of the technologies and their effectiveness in light of technological developments.

The proposal was specifically targeted at *large* user-generated platforms, and sought to impose specific, additional requirements on them. In particular, Art 13 envisages licensing, and the use of content filtering technology that would prevent infringements of content identified ahead of time by copyright owners, without those owners needing to send notices *ex post*. The proposal would leave the safe harbours in place for many entities which would presently rely on them.

Since September 2016 Article 13 has generated significant debate, which at the time of writing is ongoing.[96] Academic commentary criticized the proposal for being unclear (what is a 'large amount of works'?), and for being inconsistent with case law of the CJEU and with the fundamental rights and freedoms guaranteed by the Charter of Fundamental Rights of the EU.[97] The debate reflects the difficulty of legislating specifically to address the issue of (large) user-generated content platforms without otherwise disturbing or complicating the Article 14 safe harbour for hosting, and the scope of the communication to the public right (as to which see the case law discussion below). At the time of writing, the Council was seeking political guidance on several questions before further developing the Directive Proposal:

1. Whether the Directive should explicitly state that service providers that store and give access to user-uploaded content are directly exercising the right of communication to the public, and (if so) under what conditions (thus intervening in an area with a large and complex case law developed by the CJEU);

2. Whether such service providers should be explicitly removed from eligibility for the Article 14 safe harbour – meaning they would be liable for copyright infringements by their users;

3. Should there be some targeted mitigation of liability to avoid an excessive impact on user-generated content platforms – for example removing liability provided that the provider takes effective measures to block content identified by right holders in advance, and remove and avoid future uploads of specific identified content (notice and staydown).[98]

[96] Developments are summarised in a EU document, *Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market – Presidency Compromise Proposal and State of Play*, 13 December 2017 (Document 15651/17).

[97] Senftleben, Martin and Angelopoulos, Christina and Frosio, Giancarlo and Moscon, Valentina and Peguera, Miquel and Rognstad, Ole Andreas, The Recommendation on Measures to Safeguard Fundamental Rights and the Open Internet in the Framework of the EU Copyright Reform (October 17, 2017). Available at SSRN: https://ssrn.com/abstract=3054967 or http://dx.doi.org/10.2139/ssrn.3054967.

[98] This is reflected in the third (and current) compromise proposal of the Presidency: see ibid.

Case law

In the period since 2011 the Court of Justice of the European Communities (CJEU) has issued a number of important judgments on the scope of the safe harbours in the Ecommerce Directive, and the interaction between that directive and the Directive on Copyright in the Information Society.[99] Much of the application of the safe harbours is devolved down to national courts, resulting in some inconsistencies of approach.[100]

Eligibility for the safe harbours

A key question that has arisen is when a service provider is eligible to rely on the safe harbours established by the Ecommerce Directive. Case law establishes that an online service provider which plays an **active** role in relation to content will have knowledge of or control over the data and hence be ineligible for safe harbour protection.[101] This will apply when the service provider provides assistance to its users by, for instance, optimising the presentation of the online offers for sale or promoting those offers. A key question is whether an entity is engaged in an active, rather than a passive role.

In *L'Oreal v eBay,*[102] L'Oreal argued that eBay was not taking sufficient steps to stop the sale of counterfeits on its online marketplace. One question was whether eBay was entitled to rely on the liability exemption set out in Article 14(1) of the Ecommerce Directive in relation to the hosting of information provided by its various sellers. The case arose in the context of eBay's practice of assisting sellers, in some cases, to enhance their offers for sale, and promote and increase their sales (for example through display of advertisements through use of Google keywords). The CJEU held that in relation to a marketplace like that of eBay:

> '[T]he mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability provided for by Directive 2000/31 … Where, by contrast, the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31.'[103]

Application of this reasoning falls to national courts. Questions have arisen whether *any* optimization (including basic categorization) excludes eligibility for the article 14 Safe Harbour.[104]

---

[99] The CJEU has also issued important decisions on the scope of direct liability for the communication of copyright works. This case law is beyond the scope of this paper, but is discussed in Eleonora Rosati, 'Why a Reform of Hosting Providers' Safe Harbour is Unnecessary Under EU Copyright Law', *CREATe Working Paper* 2016/11 (August 2016). Available at:
SSRN: https://ssrn.com/abstract=2830440 or http://dx.doi.org/10.2139/ssrn.2830440.

[100] Dinwoodie above n 51.

[101] C-236/08 to C-238/08, *Google France and Google* paragraphs 113-114, 120 (23 March 2010), stating that a service provider falls outside article 14 when it 'plays an active role of such a kind as to give it knowledge of, or control over, those data'.

[102] C-324/09 *L'Oréal SA and Others v. eBay International AG and Others* § 139 [2011]

[103] ibid [115]-[116].

[104] Senftleben et al, above n 97, 16-17, criticising the original DSM Proposal for suggesting that any optimisation at all would deprive a service provider of Article 14 protection.

In the 2017 *Pirate Bay* decision,[105] the CJEU considered a request for an order that two key internet access providers in the Netherlands block access to *The Pirate Bay*. The question referred to the court was whether The Pirate Bay – which provided an index of links to infringing material, without actually hosting any infringing material – was itself communicating copyright works to the public. The Court held that the Pirate Bay was directly communicating works. The case illustrates that the case law in Europe regarding the communication right, and when it is exercised, is developing, and can take into account questions regarding the knowledge and commercial motivations of the alleged communicator. Controversy over the scope of the communication right has complicated negotiations over the Digital Single Market Directive as noted above.

The application of Article 15 and pro-active monitoring and filtering of content

A feature of the European safe harbours is that a court may award an injunction against an internet intermediary requiring them to take action to prevent infringements, even (as held recently by the CJEU in *McFadden*[106]) in the absence of any civil liability on the part of the intermediary. Such injunctions may include injunctions requiring the blocking of certain specific, infringing sites, as established by the CJEU in *Telekabel*[107] and applied in the United Kingdom in a string of cases interpreting s 97A of the *Copyright Designs and Patents Act 1988* (UK), including *Twentieth Century Fox Film Corp v British Telecommunications Plc.*[108]

A question however has arisen relating to how far such injunctions may go to requiring pro-active enforcement or filtering of infringing content, consistent with art 15 of the Ecommerce Directive, which prohibits monitoring of activity, and other principles of European law including in particular a requirement of proportionality and respect for fundamental rights of subscribers and the freedom of intermediaries to conduct legitimate business. Two cases clarify this point. In *Scarlet v SABAM,*[109] Belgian collecting society SABAM requested an (open-ended) order that a network access provider monitor and block peer-to-peer transfer of music files relating to works for which SABAM administered the relevant rights. The CJEU held that a broad order of the kind sought would both contravene the Ecommerce Directive ban on general monitoring obligations, and unduly compress users' fundamental rights.

In *Netlog,*[110] SABAM sought an order against an online social networking site which was allowing users to make use of audio works on their profiles. Again the question arose whether EU law allowed the imposition of an obligation to (preventatively) filter user posts for the relevant musical content. The CJEU held that imposing an injunction of that kind would interfere with Netlog's freedom to conduct its business, and would potentially interfere with the fundamental rights of Netlog's users. As Malovic notes however:

---

[105] *Stichting Brein v Ziggo BV and XS4All Internet BV*, C-610/15 (14 June 2017).

[106] *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH*, C-484/14, EU:C:2016:689

[107] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproducktionsgesellschaft mbH*, Case C-314/12, 27 March 2014.

[108] *Twentieth Century Fox Film Corp v British Telecommunications Plc* [2011] EWHC 1981 (Ch); also *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd* [2012] EWHC 268 (Ch); *EMI Records Ltd v British Sky Broadcasting Ltd* [2013] EWHC 379 (Ch); *Football Association Premier League Ltd v British Sky Broadcasting Ltd* [2013] EWHC 2058 (Ch); *Paramount Home Entertainment International Ltd v British Sky Broadcasting Ltd* [2013] EWHC 3479 (Ch); *1967 Ltd v British Sky Broadcasting Ltd* [2014] EWHC 3444 (Ch); *Cartier International v British Sky Broadcasting Ltd* [2014] EWHC 3354.

[109] *Scarlet Extended*, Case C-70/10 *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR I-11959.

[110] Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV* [2012] ECLI:EU:C:2012:85.

> The CJEU decisions in Scarlet and Netlog appear to have clarified that an injunction imposing blanket filtering on ISPs would be hardly considered compatible with EU law. However, neither decision has addressed whether specific forms of filtering could be instead accepted. An example might be the so called 'notice-and-stay down' system, advocated by a number of rightholders. This would require ISPs, once notified for removal, to then pursue pro-actively a 'notice and stay down' approach, so that when a piece of content has been notified for removal, it is not indexed again for the same site and stays removed.[111]

In other words, the CJEU has required that procedural protections be in place for ISP and user interests. The requirement of proportionality also 'suggests that measures appropriately imposed on one intermediary might differ from those to be implemented by another of quite different size and sophistication'.[112] Courts at the national level have, however, imposed some pro-active requirements to prevent future infringement. Thus German courts applying the *Störerhaftung* doctrine courts have imposed on intermediaries obligations to prevent future infringements of essentially the same character as those arising in the case.[113] Similar questions are also, as noted above, being aired in the discussion around the Digital Single Market Proposal.

New Zealand

New Zealand legislation remains as discussed or foreshadowed in the 2011 Paper.[114] Thus in New Zealand:

- An internet intermediary can potentially be liable for authorising copyright infringement where customers engage in copying or communicating copyright works;[115]
- An internet service provider (defined to include both carriers and hosts)[116] does not infringe copyright or authorize infringement,[117] and is not exposed to civil remedies or criminal

[111] Nedim Malovic, 'Presumed Innocent: Should the Law on Online Copyright Enforcement and ISP Liability Change?', forthcoming in *Nordiskt Immateriellt Rättsskydd*.

[112] Dinwoodie above n 51, 57-59.

[113] Dinwoodie above n 51, 52-53, citing Annette Kur, 'Secondary Liability for Trademark Infringement on the Internet: The Situation in Germany and Throughout the EU *(2014) 37 Columbia Journal of Law & the Arts* 525.

[114] New Zealand has introduced legislation in other areas of interest: in 2015, New Zealand enacted the Harmful Digital Communications Act 2015 (NZ) which provides recourse to persons who have been harmed because of the digital publication by third parties of content which was made in confidence or without their consent. It is targeted at communications that cause serious emotional distress (s 4 definition of 'harm'), such as through the sharing of intimate images. Sections 23-25 of the Act create a safe harbour from liability for 'online content hosts' (OCH). Section 24 specifics that if the process set out in that section is followed, 'No civil or criminal proceedings may be brought against an online content host in respect of the content complained of' (s24(1)), with this being subject to whether the host provides an 'easily accessible mechanism that enables a user to contact the host about specific content in the manner provided in that section' (s25(2)) and whether 'the person who provides the specific content does so on behalf, or at the direction, of the online content host' (s25(3)). Section 24 sets out various notification requirements and procedures, such as that the OCH 'provide the author of the specific content with a copy of the notice of complaint…' (s24(2)(a)(i)), and 'as soon as practicable but no later than 48 hours' after receiving a notice of complaint, the OCH should if possible, notify the author and inform them of a right to submit a counternotice' (s24(2)(a)(ii)). Failure to follow the process does not of itself create liability: s23(2).

[115] *Copyright Act 1994* (NZ) ss 16 (definition of restricted acts); 29, 30, 33 (primary infringement); s16(1)(i) (authorisation as a restricted act).

[116] *Copyright Act 1994* (NZ) s 2(1).

[117] Note that like the Canadian provision, and unlike the Australian ss 39B/112E, this exception applies to both direct and authorisation liability.

sanction, merely because another person uses their services to infringe (s 92B(2)), although injunctions may be available;[118]

- Caching does not infringe copyright, subject to the usual conditions;[119]
- Internet hosts storing material provided by users do not infringe unless they have knowledge of infringement, or reasons to believe there is infringement of copyright; or they fail to delete or remove access to material as soon as possible; or if the user is acting on their direction.[120]

New Zealand law has no exception that allows for the large-scale copying and storage necessary for the provision of internet search,[121] or text or data mining.

New Zealand also operates a system of graduated response whereby copyright owners can send notices to internet access providers and have those notices sent on to users, with the potential to escalate to a range of remedies (including monetary remedies imposed by the Copyright Tribunal) if the user continues to infringe.[122]

In June 2017 the Minister of Commerce and Consumer Affairs released a terms of reference to launch a review of the Copyright Act 1994.[123] The terms of reference do not specifically mention questions around internet intermediaries, but the planned review is a holistic one. A government study preceding the release of the terms of reference mentions frustration with the safe harbours and online infringement, although it also noted comments by some copyright owners that they had good relations with platforms and that platforms acted quickly to remove infringing material.[124]

Singapore

Legislation

Because Singapore has a post-2000 free trade agreement with the US, Singapore's copyright law in this area reflects the US position under the DMCA. Unlike Australia, Singapore implemented their

[118] *Copyright Act 1994* (NZ) s 92B(4). The provision states that it 'does not limit' the right of a copyright owner to obtain an injunction. This wording is not entirely clear but may require a showing of liability (as compared to the lack of such a requirement under European law).

[119] *Copyright Act 1994* (NZ) s 92E. The conditions are that the service provider must not modify the communication; must comply with copyright owner conditions on access; must not interfere with the use of technology that is lawful in order to obtain data on the use of the work or other subject-matter; and must update consistent with reasonable industry practice.

[120] *Copyright Act 1994* (NZ) s 92C.

[121] The *Copyright Act 1994* (NZ) s 2 defines 'internet service provider' to include a service provider who 'hosts material on websites or other electronic retrieval systems that can be accessed by a user'. This definition is on its face sufficiently broad to cover the activities of a search engine. The safe harbour itself is limited to situations where 'an Internet service provider stores material provided by a user of the service', and states that the service provider does not infringe copyright *by storing* the material – there is no mention of communicating the material (or any other activity that a search engine might undertake). This might be broad enough to cover the activities of a search engine (which does indeed store material), but is not quite the same as the EU safe harbours that have been interpreted to include search engines (which refers to a service 'that consists of the storage of information provided by a recipient of the service'.

[122] *Copyright Act 1994* (NZ) ss 122A – 122U.

[123] See http://www.mbie.govt.nz/info-services/business/intellectual-property/copyright/review-copyright-act-1994.

[124] Ministry of Business, Innovation and Employment (NZ), *Copyright and the Creative Sector* (December 2016), available at http://www.mbie.govt.nz/info-services/business/intellectual-property/copyright/copyright-and-the-creative-sector/copyright-and-the-creative-sector.pdf.

free trade agreement obligations fully. Thus there are 4 safe harbours available for (all) internet intermediaries in Singapore:

- ISPs are shielded from monetary remedies for copyright infringement for transmissions initiated by a third party, without selection by the ISP, with automatic allocation of recipients of material by the ISP and without the ISP substantially modifying the material.[125]
- Network service providers are shielded where a cache copy is made of a work through automatic processes to facilitate efficient delivery of the material to users, subject to the usual conditions.[126]
- An internet intermediary is shielded where it provides a hosting and/or referral service. The intermediary must store the electronic copy and not derive any direct financial benefit from the infringement that takes place in storage/referral, and must designate a recipient of take down notices. They will lose the benefit of the safe harbour if they do not act quickly once seized of actual knowledge.[127]

There is no need for active surveillance by an ISP of its customers' activities to identify infringement, however the service provider must have a suitable policy to deal with repeat offenders and technical measures for protecting copyright materials.

Singapore also provided the model for Australia's relatively new s 115A provision enabling courts to issue injunctions requiring internet access providers to block access to flagrantly infringing websites.[128]

A public consultation on potential amendments to the Copyright Act launched in 2016 did not include any issues relating to intermediary liability.[129]

In terms of case law, the decision of the Court of Appeal in *RecordTV Pte Ltd v MediaCorp TV Singapore Pte Ltd* [2010] SGCA 43 is important in establishing the level of risk that intermediaries are likely to face for both direct and secondary forms of copyright liability. The decision concerned a service similar to that in question in the Australian *Optus TVNow* case (that is, a cloud-based service for recording broadcast television, which individuals were allowed to do pursuant to an exception in the Act).[130] In contrast to the Australian Full Federal Court, the Singaporean Court of Appeal determined that RecordTV did not copy the broadcasts (the users did), and did not communicate the broadcasts to the public: the communications were not 'to the public' and were done by the users who had determined the content. Finally, RecordTV did not authorize any copyright infringements.[131]

---

[125] *Copyright Act 1987* (Sing) ss 193B; 252A.

[126] *Copyright Act 1987* (Sing) ss 193C; 252B. The conditions are, inter alia, the service provider must not make substantial changes to the content and if issued with a take down notice, quickly take reasonable actions to remove or restrict access to the cached copy of the work. Note that the Singapore Act has other specific provisions on user caching: s 193E, 252E.

[127] *Copyright Act 1987* (Sing) ss 193D, 252C.

[128] *Copyright Act 1987* (Sing) ss 193DDA-193DDC, introduced by the Copyright Amendment Act 2014 (Sing).

[129] See https://www.mlaw.gov.sg/content/minlaw/en/news/press-releases/public-consultation-open-for-feedback-on-singapores-copyright-re.html.

[130] above n 37, discussed above page 8.

[131] The court affirmed the earlier decision in *Ong Seow Pheng v Lotus Development Corp* [1997] 2 SLR(R) 113 which took a relatively narrow view of authorisation, holding (at [27]) that the word "authorise" meant to grant or purport to grant, whether expressly or impliedly, to a third person the right to do the act complained of, regardless of whether the intention was that the grantee should do the act on his own account or only on account of the grantor. The court in *Ong Seow Pheng* also held that authorisation could only emanate from someone having or purporting to have authority to grant the right to do the act complained of; an act was not

In summary, it appears that as compared to Australia, internet intermediaries in general in Singapore face lower legal risks of liability for copyright infringement when conducting activities like providing network access, caching, hosting and operating a search engine or similar service.

Japan

Legislation

Copyright law in Japan is governed by the Copyright Act. Also relevant to issues of intermediary liability is the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers 2001.[132] Like the European Ecommerce Directive, the Act provides horizontal protection from liability (it limits liability for 'any right of others is infringed by information distribution').[133] The purpose of the latter Act is to set forth limitations of liability for damages of specified telecommunications service providers, and to grant right holders the right to demand disclosure of identification information of the senders in case of infringement of the rights through information distribution by specified telecommunications services.

The Act shields intermediaries ('specified telecommunications service providers') from liability for infringement for transmitting materials with the aim of facilitating direct reception by a member of the public. Protection is lost if it is technically feasible for the intermediary to prevent infringing transmissions and the intermediary has actual knowledge of such transmissions or is aware of the contents of communications and could reasonably suspect infringement is taking place. Intermediaries are also shielded from loss caused to the originator because of actions taken to disable communications reasonably suspected to be infringing or when a rights holder petitions the intermediary and the originator does not contest the petition within 7 days. The Act also enables the person whose rights have been infringed to demand identifying information relating to the infringer necessary for the person demanding said disclosure to exercise his or her rights to claim damages and where there is justifiable ground for said person to receive disclosed identification information of the sender. Academic commentary comparing the Japanese legislation to the US legislation has pointed out that providers face a higher risk in Japan: 'While a provider could be held liable for failing to properly recognize infringement under the Provider Liability Limitation Act, it is held liable only in case of severe negligence under DMCA.'[134]

Japan has specific exceptions in its Act to allow internet search (articles 47*septies* and 47*octies*) and caching (article 49*quinquies*).

Cases

Japanese copyright has tended to be strict in relation to intermediaries, and readier to find that they are directly liable for copyright-infringing activities done by their users, rather than liable only for authorising infringement. A seminal case for liability of intermediaries in Japan is 1988 the *Club Cat's*

---

authorised by a person who merely enabled, possibly assisted or even encouraged another to do that act, but who did not actually have or who did not purport to have any authority which he could grant to justify the doing of that act: at [28].

[132] Act No 137 of 2001.

[133] Limitation of Liability for Damages of Specified Telecommunications Service Providers 2001 art 3(1). Note that the discussion here relies on an unofficial translation of the Act.

[134] Tomoaki Watanabe and Iwao Kidokoro, 'A World Without Cablevision nor Sony: How Japanese Courts Find Providers of Personal Locker and Content-Sharing Services Liable' (March 31, 2013). *TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy*. Available at SSRN: https://ssrn.com/abstract=2238359.

Eye case.[135] In this case, the defendant karaoke bar was held directly liable for infringement when sued by the Japanese Society for Rights of Authors, Composers and Publishers, because they had encouraged patrons to sing to copyrighted tracks and did this as part of a business.[136] In the 2001 *Video Mates* decision[137] a karaoke equipment lessor was found liable to pay royalties to same society due to the infringing actions of the lessee. The court took into account the likelihood of copyright materials being played on the equipment and the ease with which the defendant could check whether the lessee had a licence to play copyright music; this was sufficient to impose a duty of care in favour of the Society which had been breached because the lessor did not verify the existence of a licensing agreement.

Secondary infringement is also possible: in the 2005 *File Rogue* decision,[138] the defendant was found to be liable as an accessory due to its contribution to infringement of third parties, because the file sharing service it offered enabled a high volume of infringement by users, the defendant could not show that licensed files had been shared, the defendant was aware of the infringing activity and could have stopped the infringement and there was a future intention to profit from the service which was free at the time of Court assessment.

In respect of TV broadcast recording and access providers being held liable for infringement, Japanese Courts have looked at the technical setup when determining intermediary service providers liability. In the 2005 *Rokuga Net* decision, the defendant, a for-profit facilitator of transmitting Japanese broadcasts to overseas users was found to be directly liable. Notably the defendant in that case ran the entire technical set up itself. In contrast, in the 2006 *Maneki TV* case, the defendant was found not to be liable for providing a similar service because users had to purchase and remotely operate a piece of hardware to enable the service.[139] In the 2009 *Winny II* decision, a distributer who developed P2P file sharing software was found not liable for infringing activities of users, because it could not be shown that the distributor both knew of and recommended the infringing use of the software (ie the latter could not be shown).

According to some commentators,[140] a provider of some cloud-based service could be deemed a direct infringer on the *Club Cat's Eye* reasoning. Watanabe and Kidokoro argue that in Japan (in reasoning reminiscent of that of the Full Federal Court in *Optus TVNow*), providers of an online personal locker (or cloud storage) may be deemed to be performing both the act of uploading of files by users (on the basis that it is the operator's server making the copies), and downloading of

---

[135] *Club Cat's Eye/Singing at a Karaoke Lounge*, 1984 (O) No.1204 (1988) (Japanese Sup. Ct., Mar. 15, 1988).

[136] According to secondary materials on the Japanese law, 'Under Japanese law, it is not clear if one can obtain injunctive relief from indirect infringers. A copyright holder may seek both damages and injunctive relief. A damages claim is based on tort law. Article 719(2) of the Japanese Civil code provides an indirect actor's liability. In copyright cases, this provision has been applied to damages claims, but not injunctive relief. An injunctive relief claim is based on Article 112 (1) of the Copyright Act. However, it is not clear if one can obtain injunctive relief from indirect infringers. Thus, these who seek to stop an infringement often try to argue that a party that looks like an indirect infringer is actually a direct infringer. The courts tend to accept such argument': Watanabe and Kidokoro, above n134.

[137] *Supply of Karaoke Equipment for Business Use ("Video Mates" Case),* 2000 (Ju) No.222 (2001) (Japanese Sup. Ct., Mar. 2, 2001)

[138] 187 File Rogue, Heisei 16 (Ne) 446 (2003) (Tokyo High Ct., Mar. 31, 2005).

[139] 189 Maneki TV, 2006 (La) No. 10012 (Tokyo District Court, Jun. 20, 2008)

[140] Watanabe and Kidokoro, above n 134. For example, in the *MYUTA* decision, company called 'Image City' offered a service (MYUTA) whereby a user would upload his or her own music files from their personal computer to Image City's servers, and could then download music files to their cell phone for listening. The Tokyo District Court held that in these circumstances Image City was reproducing music (and hence a direct infringer in the absence of a licence): Hanji No. 1979, page 100, Tokyo District Court (5/25/2008).東京地判平成 19・5・25 判時 1979 号 100 頁, described in Watanabe and Kidokoro, above n 134.

files by the users (which could be deemed a public transmission by the cloud operator).[141] And in *Rokuraku II*, the Supreme Court considered the liability of a kind of cloud television recording service. In that case, a network-connected recording device, located in Japan, recorded Japanese TV programs and streamed them via the Internet to Japanese people living outside of Japan. The Supreme Court held that the service provider was (again, directly) responsible for making the relevant copies.[142] There has been discussion in Japan and a report considering whether amendments are needed to allow for cloud services, but no legislative action as yet.[143]

South Korea

Legislation

South Korean copyright law recognises a range of forms of liability for copyright infringement which can be applied to internet intermediaries, including liability for aiding and abetting the infringements of others.[144]

South Korea is party of a free trade agreement with both the EU and the United States, and the Korean Copyright Act implements a system for the reduction of the risk of online service provider liability broadly consistent with the EU/DMCA approach. Thus 'online service providers' are protected from infringing copyright if they fulfil certain basic conditions, when undertaking transmission (article 102(1)); caching (article 102(2)); storage at the direction of third parties (article 102(3)) and information location services or search (article 102(4)). OSPs can be informed of alleged infringement through take down procedures specified by statute (article 103)[145] and an entity which is the subject of a take-down notice may contest it (article 103(3)). As above this only provides a partial indemnity and is not available for the period where an OSP gains knowledge of the infringement prior to receiving a take-down notice. The Korean legislation *requires* an online

[141] The user's copying could be legal under article 30 of the Copyright Law of Japan: '[u]nder the Japanese copyright law, unauthorized copying of the works of others for the purpose of personal consumption (neither done as a part of work, nor shared with strangers) is fairly broadly permitted. On the other hand, if a provider engages in the act of copying, this copying is not "personal," and it is generally found illegal': Watanabe and Kidokoro, above n 134. Public transmission of copyright works is subject to the exclusive right of the copyright owner: article 23.

[142] Minshu, Vol. 65, No.1, Page 399, Supreme Court (January 20, 2012); Hanji, No. 2013, page 128.最判 平成23・1・20 民集 65 巻 1 号 399 頁、判時 2013 号 128 頁, described in Watanabe and Kidokoro, above n 134

[143] See Watanabe and Kidokoro, above n 134 for a discussion of (and criticism of) the process. A government report noted concerns about the potential of cloud providers without proposing any amendments.

[144] Soribada, 2005 Da 11626 (2007) (Sup. Ct. Rep. of Korea, Jan. 25, 2007); Soribada, 2006 La 1535 (2007) (Seoul High Ct., Oct. 10, 2007). The case involved developers of a P2P file sharing service as defendants. The court found the defendants liable due to negligence in failing to recognise the assistance provided to infringers as well as liable for aiding and abetting given that the developers were aware that there were infringing uses for the software but notwithstanding this they developed and distributed the software and facilitated copyright infringement. In subsequent litigation, the Court granted a preliminary injunction to rights holders and suggested technical measures which only allowed download of files confirmed to be licensed by the provider (in order to mitigate their liability, the Soribada developers had introduced a system which would prevent download of files in relation to which the right holder had specifically requested action).

[145] Note that in addition to the takedown provisions in the copyright law, Korea has a broader takedown system via the *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (ICNA, Information and Communications Network Act).* This provision is applied to infringements such as defamation or breach of privacy (in at least one decision a court has refused to apply it to infringement of trade mark). For more information see the World Intermediary Liability Map Project of the Center for Internet and Society at Stanford University: http://cyberlaw.stanford.edu/page/wilmap-south-korea.

intermediary immediately to suspect access to works on notification by a rightholder: intermediaries have no discretion to determine whether such notified works infringe copyright.

Notably (and in a departure from the US legislation), the Korean Act also states that 'an online service provider shall not be responsible for any infringements of copyright and other rights protected under this Act due to the reproduction or interactive transmission of works, etc. by other persons, if taking [notice and takedown and other safe harbour measures] is not technologically possible.' This additional provision has however been interpreted narrowly by the Korean courts.[146]

As under the US DMCA (and in the European system) certain orders can be made against an OSP. A provider of transmission services can be required to terminate specific accounts, and/or take reasonable measures to prevent access to specific foreign websites. Other OSPs can also be required to delete or prevent access to infringing files, and 'Other measures that the court deems necessary to the extent of imposing the minimum burden on the online service provider' (art 103bis).

The Korean legislation also contains a further enforcement tool that targets certain online service providers, aimed mainly at peer-to-peer operators and cyberlockers. Under article 104, 'An online service provider who aims principally to enable interactive transmission of works, etc. between other persons by using computers (hereinafter referred as "special types of online service provider") shall take the necessary measures such as technological measures, etc. to block illegal interactive transmissions of the works, etc. upon requests from the rights holders. In such cases, matters related to the requests from rights holders and the necessary measures shall be determined by Presidential Decree'. The *Enforcement Decree of the Copyright Act* defines those necessary measures as:

1. Technical measures capable of identifying the work, etc. by comparing the title, characteristics of work, etc. (basically, a filtering measure mainly based on the titles and hash values of the works)
2. Measures of limiting search or transmission to cut off illegal forwarding of work, etc. that came to be recognized pursuant to subparagraph 1 (basically, a keyword based measure that prevents searching of the keywords and uploading of files including the keywords);
3. Where the illegal forwarder of the relevant work, etc. is identifiable, the dispatch of warning sign wording to the forwarder of the work, etc. requesting for the prohibition of infringement on the copyright.

Failure to implement such measures can lead to a civil fine, and the service provider may be subject to cancellation or suspension of its business registration under the Telecommunications Business Act.

Korean law also contains a three strikes system for users of OSPs who are sent warnings, under the discretion of the Minister of Culture, Sports and Tourism each time transmission of infringing content is detected. After three or more warnings, a user may be suspended on ministerial order.[147]

[146] In Supreme Court Decision 2011Do1435, September 26, 2013, the defendants implemented filtering measures utilizing hash values and banned keyword lists. The Supreme Court found that those measures were not state of the art measures available and didn't work properly, and therefore the defendants could not resort to the safe harbor under Article 102(2).

[147] Korean Copyright Act articles 133-2 and 133-3.

Israel

Israeli law provides a number of bases on which an online intermediary could be held liable for copyright infringements committed by its users, including both contributory liability,[148] and via the Tort Ordinance which provides for liability for 'any person who joins or aids in, authorises, counsels, commands, procures or ratifies any act done or to be done, or any omission made or to be made, by any other person will be liable for such act or omission.'[149]

The Israeli Copyright Act contains a number of exceptions that are relevant to the conduct of an online intermediary, in particular an exception for technical acts of reproduction that is similar to the equivalent provision in Europe.[150] Israeli law also includes a fair use defence.[151]

Israel does not have any equivalent to the US/EU safe harbours in either its copyright law nor in any general (horizontal) law. Although some time ago an ECommerce Bill was proposed which would have created horizontal safe harbours for online service providers including hosting providers, and search engines, subject to certain basic conditions.[152] The Bill however did not proceed to legislation.

In several cases, however, Israeli courts have adopted the view that entities that act in accordance with a notice and takedown model will avoid liability, citing US cases. Thus in *Roter,*[153] the District Court held that a notice and take-down rule was justifiable under Israel's general law relating to contributory liability, according to which an intermediary ought not be held liable unless it had been notified of the infringement. The court cited the US decision in *Viacom v YouTube* decision holding that generalized knowledge of infringing activity ought not suffice for contributory liability, unless the intermediary was 'inducing' infringement, or if the intermediary site was essentially serves mostly for the purpose of displaying links to infringing materials. In another case, an Israeli District Court refused to order ISPs to block sites hosting software known as 'Popcorn' used to infringe copyright.[154]

---

[148] See Supreme Court, Civil Appeal 5977/07, the Hebrew University of Jerusalem vs. Schocken Publishing House (2011)**.** Contributory Liability will be recognized only when three conditions have been met: (i) there was actual direct infringement; (ii) the contributor had actual knowledge of the direct infringement; and (iii) there was substantial, significant and actual contribution by contributor to the infringement.

[149] Tort Law Ordinance, Section 12. The Tort Law Ordinance applies to infringements of copyright under s 52 of the Israeli Copyright Act 2007: see generally the World Intermediary Liability Map Project of the Center for Internet and Society at Stanford University:
http://cyberlaw.stanford.edu/page/wilmap-israel.

[150] Under s 26 of the Israeli Copyright Act 2007, transient copying, including incidental copying, is permitted if the copying is: (i) an integral part of a technological process and the only purpose of which is to enable transmission; (ii) between two parties, thorough a communication network, by an intermediary entity, or any other lawful use of the work; (iii) provided the said copy does not have significant economic value in itself.

[151] Copyright Act 2007 (Israel), s 19.

[152] Section 10 of the Bill would have prevented liability of a service provider for torts or IP infringement provided (a) the service provider did not know, when the material was uploaded, that distribution constituted a tort or IP infringement, (b) the data distributor was not acting on behalf of the service provider or subject to its control, and (c) the service provider acts to remove access to the material after receiving a complaint.

[153] C.F. 567-08-09 *A.L.I.S. v Roter Net Ltd.* See also C. F. 64054/04 *Al Hasculchen Gastronomic Center Ltd v Ort Israel*; C.F. 1559 *Chemda Gilad v Netvision Ltd.*

[154] District Court of Tel Aviv , Civil Action 37039-05-15, ZIR"A et al. vs. Anonymous, Bezeq Ben Leumi et al., July 1 2015.