

LEGISLATION NOTE

The Copyright (New Technologies) Amendment Act 2008 and New Zealand's Notice-Takedown Regime

TOM HALLETT-HOOK

On 10 July 2001, the Ministry of Economic Development published a discussion paper entitled “Digital Technology and the Copyright Act 1994”,¹ which described itself as the “first step in public consultations on copyright issues that relate to digital technology, electronic-commerce and the copyright implications of the Internet”.² After seven years and presumably a number of steps, the Copyright (New Technologies) Amendment Bill 2008 (“the Bill”), described by the Hon. Judith Tizard as “a vast, three-dimensional jigsaw”,³ was read for a third time on 3 April 2008 and passed on 8 April 2008.

The Bill, substantively amended at the eleventh hour by Supplementary Order Paper 193 (“SOP 193”),⁴ was intended to update New Zealand’s copyright law in light of modern technological developments, and the responses of other jurisdictions and the international community.⁵ The Bill’s objective was not to alter the balance between protection and access established by the Copyright Act 1994 (“Copyright Act”); rather, it was to ensure that new technologies did not upset this balance and that New Zealand’s copyright regime was technologically neutral.

To this end the Copyright (New Technologies) Amendment Act 2008 (“Amendment Act”) has amended the Copyright Act in a number of ways. Some of the most significant include: new safe harbour provisions protecting internet service providers (“ISPs”) from liability; updated permitted acts for fair dealing and educational establishments; format shifting for sound (but not video) recordings; new limited exceptions for decompilation of computer programs; and the creation of a more sophisticated technological protection measure (“TPM”) regime. This regime restricts the definition of TPM to mechanisms that prevent infringement of copyright in a work

1 “Digital Copyright and Technology Act 1994: A Discussion Paper” Ministry of Economic Development (2001) <http://www.med.govt.nz/templates/MultipageDocumentTOC___991.aspx> (at 30 September 2008).

2 Ibid [8].

3 (1 April 2008) 646 NZPD 15236 (Judith Tizard).

4 House of Representatives, Supplementary Order Paper 193, Copyright (New Technologies) Amendment Bill 2008 (1 April 2008) [“SOP 193”]. See also (8 April 2008) 646 NZPD 15417 (Christopher Finlayson) for traditional opposition complaints about eleventh hour supplementary order papers.

5 See for example the World Intellectual Property Organization Copyright Treaty, opened for signature 20 December 1996, 2186 UNTS 152 (entered into force 19 July 2002).

(excluding devices that merely control access to a work).⁶ It includes a clear statement that TPM circumvention for permitted acts is not prohibited, and a mechanism whereby a user can apply to a copyright owner for assistance when prevented from exercising a permitted act by a TPM, or where this fails, engage a “qualified person” to circumvent the TPM.⁷

Rather than attempting to provide a broad overarching assessment of the changes the Amendment Act makes to the Copyright Act, this legislation note will instead examine one piece of this “vast three-dimensional jigsaw”, namely the section 92C and section 92D ISP storage safe harbour and “notice-takedown” regime. The goal will be to assess whether or not this provision succeeds in meeting the objective of the digital copyright reform process by preserving the balance between protection and access.

ISP Liability and Notice Takedown Regimes

New Zealand’s new ISP liability provisions are set out in sections 92A–92E of the Copyright Act. The provisions are, broadly speaking, reflective of the ISP safe harbour compromise struck between the United States copyright and telecommunications industries,⁸ codified in the Digital Millennium Copyright Act 1998 (“DMCA”).⁹ The genesis of the DMCA and parallel regimes (both national and international) has been comprehensively discussed elsewhere.¹⁰ For present purposes, it is sufficient to note that the United States model contemplates a balance where ISPs are protected from the excessive copyright liability risk that they would otherwise incur as “gatekeepers” to the Internet, through a number of legislative safe harbours. The underlying idea is that requiring ISPs to take responsibility for all copyright infringement on their networks would require extensive monitoring, which would interfere with user privacy and freedom of expression, as well as dramatically increasing the cost of Internet access.¹¹ Instead, the incentive to remove infringing material is preserved by making the availability of the liability safe harbours contingent on compliance with mechanisms, such as notice-takedown, designed to ensure that infringing material brought to an ISP’s attention is dealt with efficiently.

6 The significance of this is well illustrated in the UK by *Sony Computer Entertainment v Paul Own* [2002] EWHC (Ch) 45 and in the US by *Universal City Studios, Inc v Reimerdes* 111 F Supp 2d 294 (SDNY 2000) and *Chamberlain Group, Inc v Skylink Techs Inc*, 381 F.3d 1178 (Fed Cir 2004). See generally Reichman, Dinwoodie and Samuelson, “A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works” (2007) 22 Berkeley Tech LJ 981.

7 It is debatable how effective this mechanism will be as no obligation is placed on a copyright holder to comply with a user’s request for assistance.

8 In part built upon cases such as *Religious Technology Center v Netcom On-Line Communications, Inc* 907 F Supp 1361 (ND Cal 1995) that accepted that there were good policy reasons for softening strict liability for copyright infringement in the digital world.

9 112 Stat 2860 (1998) [the “DMCA”]. Codified in: 17 USC 101, 104, 104A, 108, 112, 114, 117, 512, 701, 1201–1205, 1301–1332; 28 USC 4001.

10 See for example Zarins, “Notice Versus Knowledge Under the Digital Millennium Copyright Act’s Safe Harbors” (2004) 92 Cal L Rev 257, 262–278; Reichman, Dinwoodie and Samuelson, supra note 6, 982–994.

11 Reichman, Dinwoodie and Samuelson, supra note 6, 989.

Takedown Notices in New Zealand

In New Zealand, ISP liability is now set out in sections 92A–92E of the Copyright Act. Section 92B provides a safe harbour for ISPs in relation to secondary liability for a person’s use of their “Internet services” that infringes copyright.¹² An ISP’s “Internet services” are defined in section 92B(4) by reference to the services referred to in the section 2(1) definition of Internet service provider:

- (a) [Offering] the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing;
- (b) [Hosting] material on websites or other electronic retrieval systems that can be accessed by a user.

Branch (a) of the definition of Internet services clearly shields an ISP from liability for common infringing activity such as peer-to-peer file sharing, which falls squarely within “transmission, routing or providing connections for digital online communications”. However, branch (b) of the definition is less clear. Although an ISP is shielded from liability for A’s use of its hosting services, an ISP may still be liable for storing or caching infringing material while providing these services if it fails to fall within sections 92C–92E of the Act.

The Copyright Act’s notice-takedown regime, the focus of this article, is set out in sections 92C and 92D. Section 92C provides that an ISP is shielded from liability for infringing material it stores unless:

- It knows or has reason to believe that the material infringes copyright (s92C(2)(a)(i)); and
- Does not delete or prevent access to infringing material as soon as possible after becoming aware of it (s92C(2)(a)(ii));
or
- The user whose infringing material is stored by the ISP is acting on behalf of, or at the direction of, the ISP (s92C(2)(b)).

In addition, section 92C(3) requires that, when assessing whether an ISP knows or has reason to believe that material infringes copyright in a work, a court must take into account whether the ISP has received a section 93D notice of infringement in relation to the material. The requirements

¹² Although s 92B(3) of the Copyright Act 1994 makes it clear that an ISP may still be subject to injunctive relief in relation to it, or its user’s copyright infringement.

of this notice are to be set by regulations, which at the time of writing are yet to be made.¹³

It is clear that under section 92C(a)(i) either actual or constructive knowledge will be sufficient to dislodge an ISP from the section 92C safe harbour. Smellie J examined the meaning of “reason to believe” in the context of section 35 of the Copyright Act in *Husqvarna Forest and Garden Ltd v Bridon NZ Ltd*,¹⁴ applying the following passage from the leading United Kingdom case of *LA Gear Inc v Hi-Tec Sports Plc*:¹⁵

‘[R]eason to believe’ must involve the concept of knowledge of facts from which a reasonable man would arrive at the relevant belief. Facts from which a reasonable man might suspect the relevant conclusion cannot be enough. Moreover, as it seems to me, the phrase does connote the allowance of a period of time to enable the reasonable man to evaluate those facts so as to convert the facts into a reasonable belief.

Smellie J also clarified that the appropriate question to ask is whether the defendant knew the relevant facts to determine whether a work infringed copyright. A lack of knowledge based on an error of law is no excuse.¹⁶

By way of comparison, the DMCA’s storage safe harbour, in section 512(c), also excludes ISPs¹⁷ who have actual or constructive knowledge of infringing material or activity. It further imposes an obligation, upon obtaining such knowledge, to expeditiously remove the infringing material.¹⁸ However, unlike section 92C, section 512(c) also excludes an ISP that derives a financial benefit directly attributable to the infringing activity where the ISP has the right and ability to control this activity.¹⁹

On top of these requirements section 512(c) also includes a notice-takedown mechanism.²⁰ Unlike a New Zealand section 92D notice, which is fed directly into an ISP’s knowledge of infringement, a DMCA takedown

13 The Ministry of Economic Development suggests that these regulations are likely to simply set out a prescribed form for s 92D notices. See “FQ&As about the Copyright (New Technologies) Amendment Bill” Ministry of Economic Development (2008) <http://www.med.govt.nz/templates/Page_____35261.aspx> (at 30 September 2008) [“FQ&A”]. In the US a takedown notice requires (i) identification of the copyrighted work or a representative list of multiple works; (ii) identification of the infringing material; (iii) information that reasonably allows the ISP to locate the infringing material; (iv) the complainants’ contact information; (v) a physical or electronic signature of the complainant; (vi) a statement of good faith that the use of the material is not authorized; (vii) a statement under penalty of perjury that the notice is accurate. See 17 USC 512(c)(3).

14 [1997] 3 NZLR 215 (HC).

15 [1992] FSR 121, 129 (CA) per Morritt J.

16 On this point Smellie J cited *International Business Machines Corp v Computer Imports* [1989] 2 NZLR 394 (HC), 407, 418.

17 The DMCA refers to Online Services Providers; the term ISP is used here for the purpose of convenience.

18 DMCA, supra note 9, s 512(c)(1)(A)(i)-(iii). The s 512(c)(1)(A)(ii) constructive knowledge provision was referred to in the DMCA’s legislative history as the “red flag” test. See *Reno v ACLU* 521 US 844 (1997), 880.

19 DMCA, supra note 9, s 512(c)(1)(B)(ii). For a good discussion of the difficulties the US courts have encountered determining what constitutes a “direct financial benefit” see Brown, “Annual Review 2008: Intellectual Property: Copyright: Note: Fortifying the Safe Harbors: Reevaluating the DMCA in a Web 2.0 World” (2008) 23 Berkeley Tech LJ 437, 450–458.

20 DMCA, supra note 9, s 512(c)(1)(C).

notice, if procedurally valid, obliges an ISP to expeditiously remove or disable the alleged infringing material or lose the benefit of the section 512(c) safe harbour.²¹ This obligation exists regardless of whether the material is actually infringing.²²

This notice-takedown mechanism is intended to be balanced by the section 512(g) “put-back” provision. The “put-back” provision operates by providing an ISP with a safe harbour from liability to its customers for wrongfully taking down material, provided that section 512(g) is complied with. Under section 512(g)(2) an ISP must notify an alleged infringer that their material has been removed or that access has been disabled. Once the alleged infringer is notified that their material has been removed, they may give a counter notice to their ISP.²³ The ISP is then required to forward this counter notice on to the copyright complainant. If the complainant does not file proceedings against the alleged infringer within ten working days of receipt of the counter notice the ISP must replace the alleged infringing material within the next four working days or lose its section 512(g) safe harbour. Provided that the ISP continues to operate within the boundaries of section 512(g), section 512(g)(4) gives the ISP immunity from liability for copyright infringement in relation to its replacement of the material identified in the complainant’s takedown notice.

The DMCA notice-takedown mechanism, if followed faithfully by an ISP, largely removes the need for an ISP to make its own judgement about the infringing material. Whether this is a good thing is debatable: the DMCA notice-takedown mechanism has been criticized for resulting in *ex ante* takedown that lacks due process and has a chilling effect where risk-averse ISPs are quick to remove alleged infringing material.²⁴ There is also evidence that section 512(c) and (d) takedown notices are abused by copyright holders for illegitimate purposes, such as creating leverage in a competitive marketplace; protecting rights not given by copyright; and stifling criticism, commentary, and fair use.²⁵ Problematically, the section 512(g) “put-back” mechanism has also proven less effective than anticipated because many ISPs use their terms of service to limit their

21 An ISP can refuse to comply with a takedown notice and forgo safe harbor protection if it believes the material identified in the notice is clearly not infringing. However, predictably, few ISPs take up this option as there are strong incentives not to stray from the DMCA’s takedown, put-back path. See generally Urban and Quilter, “Efficient Process or ‘Chilling Effects’? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act” (2006) 22 Santa Clara Computer & High Tech L.J. 621.

22 It is worth noting that s 512(f) of the DMCA, *supra* note 9, provides a “defence” of knowing material misrepresentation that applies to notices and counter-notices. However, arguably this “defence” is of limited use as it sets a very high bar, especially when contrasted to the relative simplicity of the takedown notice mechanism. See Urban and Quilter, *ibid* 689–690. See also Williams, “The Truth and the ‘Truthiness’ About Knowing Material Misrepresentations” (2007) 9 NC J.L. & Tech 1.

23 DMCA, *supra* note 9, s 512(g)(2)(B).

24 Urban and Quilter, *supra* note 21, 687.

25 *Ibid*. See also “Submission to the Commerce Select Committee on the Copyright (New Technologies and Performers’ Rights) Amendment Bill 2006” InternetNZ (2007) <<http://www.internetnz.net.nz/issues/submissions/archive/2007/copyright/>> (at 6 October 2008) 10 and Pollak “Rebalancing Section 512 to Protect Fair Users from Herds of Mice – Trampling Elephants, or a Little Due Process is Not Such a Dangerous Thing” (2006) 22 Santa Clara Computer & High Tech L.J. 547.

liability for removal of material, which undermines the incentives created by the section 512(g) safe harbour.²⁶

Comparing the DMCA and Copyright Act takedown mechanisms, a section 92D notice imposes a heavier burden on an ISP than its DMCA equivalent. Section 92C retains knowledge standards similar to the DMCA that, as under the United States regime, are presumably intended to lessen an ISP's obligation to positively monitor information it stores for copyright infringement. This shifts the burden of initial identification of this material onto copyright holders who are more readily able to identify potential infringements of their own copyright material.²⁷ Unlike the DMCA model, a section 92D takedown notice does not automatically oblige an ISP to "expeditiously" remove the allegedly infringing content to retain its safe harbour protection. Rather, the allegation of infringement is fed into the calculation of whether the ISP has actual or constructive knowledge that material is infringing copyright. Matters are further complicated by the fact that the Copyright Act does not provide ISPs with immunity for wrongfully deleting or preventing access to a user's stored material. This places an ISP who receives a section 92D notice in the unenviable position of having to make a determination of whether the allegations of copyright infringement warrant the deletion or removal of an individual's material. A decision to remove exposes the ISP to potential liability to the individual in contract or tort, while a decision not to remove potentially costs them their safe harbour protection.

As the United States experience illustrates, forcing ISPs to take a more analytical approach to removal of material in response to a takedown notice is, in principle at least, not necessarily a bad thing. However, it remains to be seen whether the New Zealand section 92D will work in practice. One risk is that ISPs, faced with the prospect of having to make difficult decisions about infringing material, will simply amend their terms of service to avoid liability for deleting or removing a user's material and adopt a precautionary approach to takedown notices where most are complied with, similar to the DMCA model.²⁸ This would have particularly serious consequences for New Zealand Internet users as there is no statutory "put-back" mechanism for a user to dispute a takedown notice, although section 92C(4) requires an ISP to notify a user that their content has been removed.

Interestingly, the Ministry of Economic Development states that once an ISP decides to remove content and notifies a user of this decision, "[w]hether the material in question is returned to the website or access to the material allowed by the ISP becomes a matter for the user and copyright owner to resolve."²⁹ It is unclear why the Ministry considers that

26 Urban and Quilter, *supra* note 21, 629.

27 See Zarins, *supra* note 10, 274.

28 Compare with the Consumer Guarantees Act 1993, for non-business customers.

29 Ministry of Economic Development, FQ&A, *supra* note 13.

once an ISP has removed infringing material it no longer plays any part in this process, since, despite the lack of a “put-back” mechanism, a user remains free to argue that the ISP’s “knowledge” of infringement is based on a mistaken understanding of fact or law.³⁰ However, pragmatically it must be acknowledged that a user is likely to find it difficult to reverse an ISP’s decision on infringement, as he or she is unlikely to have as much leverage over their service provider as an aggrieved copyright holder with the weight of the Copyright Act and the safe harbour incentive behind them. This is especially true if the ISP is risk-averse³¹ and has limited its liability for removal of its user’s content.³² This risk of copyright holder overreach is compounded by the fact that the proposed section 92CB (which made knowing or reckless authorization of a false or misleading section 92D notice an offence) was removed by SOP 193³³ leaving an ISP’s judgement as to whether material is infringing copyright as the main check on overreach through overly broad or badly-construed copyright holder takedown notices.³⁴

This suggests that it is important that ISPs are encouraged to exercise their infringement assessment function effectively and that secondary liability for an assessment of infringement that ultimately turns out to be incorrect is not too quickly imposed. This is especially true as there are strong public policy arguments against holding ISPs to a high standard of liability for secondary infringement,³⁵ suggesting that courts should be slow to impose investigative duties on ISPs under the section 92C knowledge requirements.³⁶ Furthermore, it is important to view a section 92D notice and the allegations it contains as creating a duty for the ISP to investigate the alleged infringement of copyright, rather than as immediately giving rise to actual knowledge of infringement. Where appropriate, a margin of appreciation should be retained for ISPs that, on the facts available to them at the time of investigation, reach a conclusion that material does not infringe that subsequently proves to be incorrect. This appears consistent

30 For example, by arguing that they fall within one of the Copyright Act’s fair dealing exceptions.

31 Arguably, an ISP’s willingness to stand up to ill-conceived takedown notices could become a point of market differentiation. However, it is unclear whether this issue would be significant enough to make running the risk of becoming embroiled in expensive copyright litigation worthwhile.

32 Of course, it is possible to imagine scenarios where this situation would be reversed: a small copyright holder may complain about infringing material stored by a large organization.

33 SOP 193, *supra* note 4.

34 Ministry of Economic Development, FQ&A, *supra* note 13, suggests that the Fair Trading Act 1987 and Crimes Act 1961 protect against fraudulent use of the Copyright Act’s takedown notice provisions.

35 See for example Ludwig “Shooting the Messenger: ISP Liability for Contributory Copyright Infringement” [2006] BC Intell Prop & Tech F 110701.

36 See for example *Perfect 10 v CCBill*, where the Ninth Circuit suggested pursuant to the s 512(c)(1)(A)(ii) “red flag” constructive knowledge requirement in relation to a password-hacking website known to the Defendant that “[i]here is simply no way for a service provider to conclude that the passwords enabled infringement without trying the passwords, and verifying that they enabled illegal access to copyrighted material. We impose no such investigative duties on service providers. Password-hacking websites are thus not *per se* ‘red flags’ of infringement.” See *Perfect 10 v CCBill*, 488 F 3d 1102, 3569–3570 (9th Cir, 2007) [“*Perfect 10 v CCBill*”]. It should be noted that in *Perfect 10 v CCBill* the Court also found that the plaintiff’s DMCA takedown notices were not valid and so could not be taken into account in relation to the Act’s knowledge requirements.

with the High Court's approach to "reason to believe" in *Husqvarna* as set out above. In this regard, it is unfortunate that an ISP only has an obligation to communicate with an alleged infringer once his or her material has been removed,³⁷ since in many cases where infringement is unclear, best practice would be to approach the user for an explanation or justification of the content before reaching a decision as to whether or not it should be deleted.³⁸

Another issue is whether a notice that does not comply with the section 92D requirements should be taken into account in determining an ISP's knowledge of infringement. Under the United States model, a section 512(c)(3)(B) takedown notice that fails to comply substantially with the elements prescribed in section 512(c)(3)(A) is not taken into account for the purposes of determining ISP knowledge.³⁹ The Copyright Act contains no such provision and it is unclear whether the section 92D regulations will clarify this matter. Given the investigative duty a section 92D notice imposes on an ISP and the fact that a mistaken interpretation of the law will not shield an ISP from liability, there is a policy argument to be made that once a statutory mechanism for notice of copyright infringement is in place, it would be appropriate to disregard non-compliant notices provided to an ISP when determining an ISP's knowledge of infringement. This is on the basis that a non-compliant notice fails to provide the ISP with an appropriate level of information to identify and assess an alleged infringement.⁴⁰

Conclusion

Overall, it is debatable whether the Copyright Act's new notice-takedown mechanism will preserve an appropriate balance between access and protection. Although in principle section 92C should require ISPs to take a harder look at whether alleged infringing material actually infringes, in practice there appear to be strong incentives for an ISP to err on the side of caution and remove material even where infringement is questionable. Given the ease with which copyright holders can allege infringement through a section 92D notice, there is a risk that the balance between access and protection will be skewed in their favour. Whether or not this turns out to be the case will depend in part how other pieces of the "jigsaw" that is the Copyright Act fit together. However, what is clear is that a key factor in New Zealand's notice-takedown regime will be the willingness of ISPs to stand up for the rights of their users. It remains to be seen whether this will occur.

37 Copyright Act 1994, s 92C(4).

38 Arguably it would also be desirable for the courts to take a bifurcated approach to the question of s 92C knowledge of infringing material for the purpose of remaining within a safe harbour, and knowledge for the purposes of secondary infringement. For a discussion of this point in the US context see Zarins, *supra* note 10. Although compare the New Zealand approach to "reason to believe".

39 See for example *Perfect 10 v CCBill*, *supra* note 36.

40 This will, of course, depend on what the s 92D regulations actually require.