JAMES CARTER

STRICT LIABILITY WITHIN THE COPYRIGHT (INFRINGING FILE SHARING) AMENDMENT ACT 2011

Submitted for the LLB Honours Degree

Faculty of Law

University of Wellington

2013

Abstract

This paper examines strict liability within the Copyright (Infringing File Sharing) Amendment Act 2011. Prior to the act, enforcing copyright infringement by file sharing was unrealistic due to detection, evidentiary and authorisation problems. The Act resolved these problems by imposing strict liability in the form of vicarious liability and evidentiary presumptions. First, it explores the decision to hold account holders vicariously liable for end user infringements in relation to policy considerations and fact patterns arising in Copyright Tribunal decisions. In doing so, it highlights ways in which injustice may be avoided. Second, it explores the evidentiary presumptions, the underlying policy rationale for their inclusion and the Copyright Tribunal's application of them. Ultimately, it argues that there is good reason to remove the evidentiary presumptions.

Key Words: *File Sharing, Copyright (Infringing File Sharing) Amendment Act 2011, Copyright Tribunal, Vicarious Liability, Evidentiary Presumptions.*

Table of Contents

I Introduction 4

A Peer-to-Peer: A data dissemination revolution 4

B Claims in absence of the Act 6

C Approach of this paper 7

D The Act's regime 8

II Provisions Which Prescribe Vicarious Liability 9

A Strict vicarious liability 9

B Policy rationale for vicarious liability 11

III Provisions which Temper Vicarious Liability 13

A Tribunal discretion to include end user infringers as part of proceedings 14

B The manifestly unjust provision 15

1 Wi-Fi hackers: claims of unauthorised use 15

2 Technological incapacity and inadvertent infringement 19

C Absence of account holder 22

D Determination of award sum 25

E Flagrancy of infringement 27

IV The Evidentiary Presumptions 29

A Reading section 122N(1) as imposing strict liability 29

B Policy rationale for evidentiary presumptions 30

V Rebutting the Evidentiary Presumptions 32

A The standard required to engage section 122N(2) 32

B The standard required to engage section 122N(3) 35

C Case for removing presumptions 37

VI Conclusion 38

VII Bibliography 40

I Introduction

A Peer-to-Peer: A data dissemination revolution

Throughout history technological advancements have challenged intellectual property law. In particular, the evolution of information dissemination technology has provoked legislative response. For example, the printing press' capacity for relatively cheap, ubiquitous and uniform information dissemination prompted various reforms. In 1662, it inspired the Licensing of the Press Act, designed to supress the printing of seditious material.[1] [2] Later, in 1710, as political tolerance grew and the need for economic incentive was realised, the printing press encouraged the Statute of Anne, "the first copyright statute ever passed by a legislature".[3] [4]

Now in 2013, Peer-to-Peer (P2P) file sharing software can be couched as the most recent innovation in dissemination technology which requires legislative response. If differs from the conventional client-server method of internet information dissemination in which users download entire files from a centralised server, usually in the form of a website.[5] Where this system is used for copyright infringement, the party hosting the server offers a

[1] Licensing of the Press Act 1662 (UK) 14 Car c 33.
[2] Raymond Astbury "The Renewal of the Licensing Act in 1693 and its Lapse in 1695" (1978) s5-XXXIII Library 296 at 296.
[3] The Statute of Anne 1710 (UK) 8 Anne c 33.
[4] Thomas Morris "The Origins of the Statute of Anne" (1962) 12 Copyright L Symp (ASCAP) 222 at 222.
[5] William Hosch "client-server architecture" (February 19 2009) Encyclopaedia Britannica <www.britannica.com>.

pragmatic defendant. The on-going legal pursuit of Megaupload by United States authorities is an example of action taken against servers hosting infringing material.[6]

Conversely, P2P software fragments files, such as copyright protected digital media like music, and enables many different users to share these fragments.[7] This decentralises downloading, yielding no single easily identifiable party to pursue in a copyright infringement case. Furthermore, most P2P software employs a default function whereby the file being downloaded is simultaneously uploaded to other users. Once downloaded, unless removed, a file may remain uploading. This function has been highlighted by the High Court of Australia.[8]

Thus, when one downloads copyrighted material using BitTorrent they are not only liable for copying that work but also, usually unwittingly, of communicating that work to thousands of potential uploaders. The P2P method of file sharing is pervasive. Studies reveal it has led to copyright law being "infringed hundreds of millions of times per day around the world."[9] In New Zealand, 779,000 people are estimated to participate in illegal file sharing each month.[10] The Copyright (Infringing File Sharing) Amendment Act (the Act) represents a legislative response to file sharing software.

[6] See Toby Manhire "Kim Dotcom and Megaupload: a timeline" *New Zealand Listener* (online ed, 29 August 2013)
[7] William Hosch "P2P" (February 19 2009) Encyclopaedia Britannica <www.britannica.com>.
[8] *Roadshow Films v iiNet* [2012] HCA 16 at [21].
[9] Alexandre Mateus and Jon Peha "Quantifying Global Transfers of Copyright Content using BitTorrent" (6 September 2011) Social Science Research Network <www.ssrn.com> at 36.
[10] *RIANZ v Telecom NZ 3728* [2013] NZCOP 8 at [28].

B Claims in absence of the Act

A copyright owner could detect P2P infringement through detection services like MarkMonitor. These detection methods are limited as they can only identify Internet Protocol (IP) addresses.[11] IP addresses could be traced back to the Internet Service Provider (ISP) who assigned it to the account holder. An ISP may be required by an interlocutory order to reveal the contact details of the account holder using the infringing IP address so that a copyright owner may initiate proceedings.[12] To establish liability the copyright owner would have to show evidence that the account holder in fact infringed either by 'copying' (via downloading) or by 'communicating' (via uploading) the work per s 16(1)(a) or s 16(1)(d) of the Copyright Act 1994. This would involve climbing complex evidentiary hurdles inherent in file sharing. Whether simply pointing to the detection techniques used by the copyright owner would satisfy this factual inquiry is unknown.

Furthermore, the customer may claim that they themselves did not commit the infringing act, rather an end user of their account did. The copyright owner would then have to prove that the account holder authorised the infringing act per s 16(1)(f) of the Copyright Act, or pursue a separate action against the end user. An action against the end user would encounter detection difficulties, as the only practical means of identifying infringement is through the account holder's IP address. Coupled with litigation fees, this uncertainty has chilled file sharing copyright enforcement.

[11] InternetNZ "FAQs: Won't copyright owners only go after people who do a lot of downloading?" 3strikesnz <www.3strikes.net.nz>.
[12] District Court Rules, r 5.1.3.

C Approach of this paper

This paper will examine the Act's attempts to overcome these authorisation, detection and evidentiary hurdles by imposing two elements of strict liability in the form of vicarious liability and evidentiary presumptions. Under the Act's regime an account holder is vicariously liable for the file sharing infringing activities of the end users of his or her account. This nullifies concern regarding proving authorisation on the part of the account holder in the case of end user infringement. The Act also provides for evidentiary presumptions in favour of the copyright owner. This negates concerns surrounding the evidentiary hurdles in finding liability and expedites the process by eschewing costly and time consuming evidentiary disputes.

The first part of this paper will examine vicarious liability within the Act. It will delineate the provisions which prescribe vicarious liability and explore underlying policy considerations. It will then inspect the Copyright Tribunal's (the Tribunal) interpretation of provisions which potentially temper vicarious liability in relation to certain fact patterns arising in Tribunal proceedings. These provisions consist of the discretion to include end users in proceedings, the manifestly unjust exception and penalty sum determination. It will offer recommendations as to amendments and Tribunal approaches which could reduce potential injustices brought about by vicarious liability.

The second part of this paper will closely examine the evidentiary presumptions provided by s 122N in conjunction with the Tribunal's interpretation and application of this section. It will argue that s 122N, when read together with s 122O, can be understood as imposing

strict liability on the account holder as all factors necessary to establish liability are presumed. The policy of this dynamic will be considered. It then will examine the degree of this strictness by examining the interplay between s 122N(2) and s 122N(3), which, respectively, allow for the presumptions to be rebutted and that rebuttal itself to be refuted. Ultimately, it will be argued there is good reason to remove these presumptions.

D The Act's regime

Broadly speaking, the Act established a sui generis 'three strikes' regime governed by the Tribunal which functions as such: copyright owners hire independent contractors, usually MarkMonitor, to detect the IP address at which the infringements occur. [13] The copyright owners then pass this information on to ISPs (who are referred to as Internet Protocol Address Providers under the Act).[14] Using this information, ISPs are bound to issue up to three infringement notices to the account holder possessing the IP address; a detection, warning and enforcement notice.[15] After an enforcement notice is issued, the copyright owner may seek an order from the Tribunal for an award of a sum up to $15,000 payable by the account holder.[16] To date, every single applicant at the Tribunal has been the Recording Industry Association of New Zealand (RIANZ), a trade-association dominated by the New Zealand based subsidiaries of the 'big three' international music labels.[17]

[13] See *RIANZ v TCLE[A]-T5877102* [2013] NZCOP 2 at [21]; *RIANZ v CAL2013-E000614* [2013] NZCOP 3 at [14]; *RIANZ v Telecom NZ 3553* [2013] NZCOP 6 at [13].
[14] Copyright (Infringing File Sharing) Amendment Act 2011, s 122B(2).
[15] Ibid, s 122B(3).
[16] Ibid, s 122B(4)(a).
[17] "About RIANZ: Full Members" rianz <rianz.org.nz>.

II Provisions Which Prescribe Vicarious Liability

A Strict vicarious liability

The Act defines "infringement" as "an *incidence of file sharing* that involves the infringement of copyright in a work by a *user*" (emphasis added).[18] This definition is significant for two reasons.

First, the word 'user' clarifies that an account holder need not commit the infringing act; it may be an end user. When coupled with s 122O(1)(a)(ii), which only requires that the infringement occurred at an IP address of the account holder, this holds the account holder liable for the actions of the end user; that is, it imposes vicarious liability.

Secondly, the Act's definition of infringement could be read as imposing a form of strict liability, the form of which does not require intention but only fault. It requires only 'an incidence of the file sharing that involves infringement'. File sharing may be used for legal means and a user who recklessly infringes in the course of file sharing is just as liable, under this definition, as those who intentionally infringe.

The account holder is subject to the penalties and obligations arising in the case of an infringement. Section 122O(1) stipulates that "the Tribunal must order an account holder to pay a sum" where certain conditions are satisfied. Section 122D requires that an ISP must issue a detection notice to an "account holder" where an alleged infringement is

[18] Copyright (Infringing File Sharing) Amendment Act 2011, s 122A(1).

matched with the account holder's IP address.[19] It also provides for the form of the notice, requiring that the consequences to the "account holder" of further infringement are made clear.[20] Likewise, information on how the "account holder" can challenge the notice must be included.[21] No reference is made to the actual infringer.

The following sections, 122E and 122F, follow a similar pattern to s 122D. However, a peculiar anomaly exists. Section 122E(2)(e) specifies that a warning notice must "identify any other alleged infringements *by the account holder* against that rights owner that have occurred since the date of the preceding detection notice" (emphasis added). In contrast, s 122F(2)(e) provides that an enforcement notice must "identify any other alleged infringements *against the rights owner* that have occurred since the date of the preceding detection notice" (emphasis added).

If s 122E(2)(e) is read literally, the second infringement notice, the warning notice, only need reference infringements carried out by the actual account holder. Whilst the third notice, the enforcement notice, must refer to all other infringements carried out under that IP address, since "against" is open and may include vicarious infringement on the part of an end user. This anomaly is softened by the fact that an ISP is still bound to issue a warning notice in the case of end user infringement per s 122E(1), but s 122E(2)(e) suggests warning notices need not identify any infringements by non-account holders. This incongruity has not been addressed by the Tribunal and, as there is no discernible reason for a discrepancy between notices, it may be attributed to a drafting error.

[19] Ibid, s 122D(1).
[20] Copyright (Infringing File Sharing) Amendment Act 2011, s 122D(2)(e).
[21] Ibid, s 122D(2)(d).

Section 122G provides that it is the account holder, not the actual infringer, who may challenge the notice.[22] Likewise ss 122I and 122J clarify that, upon the issuing of an enforcement notice, the copyright owner may only take action against the account holder, as opposed to the actual infringer, in requesting the penalty fee and the amount of such a sum.[23] Section 122L(e) allows the Tribunal to consider any timely submissions by the account holder, before the proceedings. Again, no reference is made to the end user.

B Policy rationale for vicarious liability

As discussed, the base reason for vicarious liability is that it eschews the authorisation and detection obstacles and allows for realistic copyright enforcement action in the file sharing context. Vicarious liability also appears to be the most expeditious means of educating "the public about illegal file-sharing"; a routinely cited purpose of the Act.[24] Indeed, many submissions by respondents in Tribunal proceedings illustrate such ignorance on the part of end users.[25] Account holders are the only detectable party and are in a position to regulate the use of their internet account. They essentially become agents of the state responsible for deterring infringing file sharing.

However, to qualify as fair policy, this imposition of vicarious liability should require something beyond convenience. In employment vicarious liability, an employer is liable for economic reasons. Employers have the deepest pockets and derive benefit from

[22] Ibid, s 122G(1).
[23] Copyright (Infringing File Sharing) Amendment Act 2011, s 122I(1).
[24] (22 April 2010) 662 NZPD (accessed online).
[25] *RIANZ v Telecom NZ 2592* [2013] NZCOP 1 at [9]; *RIANZ v CAL2012-E000627* [2013] NZCOP 9 at [18].

employee actions.[26] In most settings it is safe to infer that an account holder has the deepest pockets as they pay the bills. However, significant exceptions exist, such as flatting arrangements. Furthermore, an account holder gains no benefit from end users' use.

It could be argued that by contracting with an ISP an account holder is deemed to have assumed responsibility for all actions undertaken on that account. This is substantiated upon examination of contracts between ISPs and account holders which render the account holder liable for data usage fees, even that usage arising from unauthorised use.[27] This imposition of responsibility in the context of infringing file sharing may be likened to minor driving offenses. The owner of a vehicle may be found liable for parking and speeding offenses committed through the use of their vehicle by other people. [28] Parliamentary debate during the passage of the Bill involved allusions to the rights and corollary responsibilities of drivers.[29] The RIANZ has repeatedly compared the Act's regime to land transport offenses in its submissions.[30]

Vicarious liability of a vehicle owner in a land transport context can be rationalised by a clear assumption of responsibility. When an owner passes over the keys they are deemed to assume responsibility for certain speeding and parking offenses committed by the

[26] Kartikey Mahajan "Corporate Criminal Liability: Why Corporations are Preferred and Not the Employees?" (6 May 2010) Social Science Research Network <www.ssrn.com> at 18-19.
[27] see "Telecom Broadband terms and conditions" Telecom NZ <www.telecom.co.nz> at cl 9 and; "Orcon Terms and Conditions" Orcon <www.orcon.net.nz> at cl 5.1.
[28] see Land Transport Act 1998, ss 133 and 133A.
[29] (12 April 2011) 671 NZPD (accessed online).
[30] see *RIANZ v TCLE[A]-T5877102* [2013] NZCOP 2 at [83]; *RIANZ v Telecom NZ 3553* [2013] NZCOP 6 at [41]; *RIANZ v CAL2012-E000627* [2013] NZCOP 9 at [77].

driver. This is evidenced by discretion to pardon the owner where possession was lost through theft, as in this case no assumption has taken place.[31]

This assumption of responsibility on the part of account holder in regards to end user activity is not as clear. No 'passing of the keys' moment exists. Arguably, the account holder's signing of a contract with an ISP assumes the responsibility for all activities undertaken under the resulting internet account. However, as most contracts' formation pre-date the passage of the Act, this deemed assumption is retrospective in many cases. Regardless, it is not a salient assumption of responsibility pertaining to end user copyright infringement. This could be remedied through an advertisement campaign outlining an account holder's responsibilities. Continued use could be perceived as consent to this advertised assumption. Parliament could also allow for the amendment of the parties to ISP contracts to address flat settings where a single tenant has taken responsibility. This would ensure account holder's clearly assumed responsibility for copyright infringing activities.

III Provisions which Temper Vicarious Liability

Certain fact patterns have arisen in Tribunal proceedings which illustrate the potential for injustice of vicarious liability in the file sharing context. These will be discussed in relation to provisions which the Tribunal could have utilised in order to ameliorate this injustice.

[31] see Land Transport Act 1998, s 269 of LTA (2)(a)(iii).

A Tribunal discretion to include end user infringers as part of proceedings

Section 122K(3) stipulates the default parties to proceedings before the Tribunal are the applicant rights owner and the respondent account holder. Section 122K(3)(c) provides the Tribunal with the discretion contained in s 212(2) the Copyright Act 1994. This entails the ability to direct a person to be joined to the proceedings where the Tribunal is satisfied that said person has "a substantial interest in matter".

In [2013] NZCOP 10, it was submitted that the relevant infringements were committed by a resident of respondent's address who was willing to take responsibility for the infringement.[32] The Tribunal responded by stating that the Act clearly makes the account holder responsible, per s 12O(1), implying it is bound to issue the penalty to the respondent.[33]

The Tribunal chose not to exercise its discretion under s 122K(3)(c) to include the resident of the respondent as a part of the proceedings. The resident indubitably had "a substantial interest in the matter" per s 212(2) of the parent Act, as he or she had taken responsibility for the infringement and it is likely that the penalty will be privately passed on to him or her.

However, as s 122O(1) makes clear, the penalty fee may only be attributed to the account holder. The Act provides no authority for the Tribunal to transfer liability for the awarded

[32] *RIANZ v Telecom NZ 4296* [2013] NZCOP 10 at [17].
[33] Ibid at [18].

sum from the account holder to the infringing end user. The Tribunal has no means of ensuring this private transfer of the penalty fee takes place.

Section 122K(3)(c) was probably included for educational purposes as it is not accompanied with the authority to charge infringing end users. In the context of minor land transport offenses, discretion exists to charge either the person who allegedly committed the offense or the owner of the vehicle.[34] The Act should provide similar discretion where an end user admits to the infringing act.

B The manifestly unjust provision

Section 122O(5) provides the Tribunal with broad discretion to decline to award the copyright owner a fee payable by the account holder if they consider such payment would be manifestly unjust to the account holder. The Tribunal dismissed judicial precedent regarding the meaning of 'flagrancy' due to the quasi-judicial nature of the Tribunal.[35] It could be inferred that the same applies to judicial authority on 'manifest injustice'. To date, the Tribunal has yet to satisfy s 122O(5), despite facts which indicate manifest injustice.

1 Wi-Fi hackers: claims of unauthorised use

The decision in [2013] NZCOP 1, 7 and 13 involved submissions by the respondent which inferred that an unauthorised third party, such as a Wi-Fi hacker, was responsible for the

[34] See Land Transport Act 1998, ss 133(1) and 133A(1).
[35] *RIANZ v CAL2013-E000614* [2013] NZCOP 3 at [34].

infringing activity.[36] In each case, the Tribunal held these allegations were insufficient to engage s 122O(5).[37] If these allegations were true, the Tribunal's refusal to engage s 12O(5) would contradict the ordinary meaning of 'manifestly unjust'. It is demonstrably unfair to hold an account holder liable for the actions of an illegal actor whom they exercise no control over. Perhaps this accords with the educative intent of the Act, as it would incentivise the strengthening of Wi-Fi security. However, the Tribunal has not discussed this policy. Instead, it dismissed these claims on evidentiary grounds.

In [2013] NZCOP 1 the respondent admitted to the infringements prompting the first two infringement notices, but denied the third through an implication of unauthorised use by a third party.[38] It was open for the Tribunal to reject the respondent's unsubstantiated claim on the grounds that she had already admitted to previous infringements of the same song and had file sharing software installed.[39] It is likely the default uploading function caused the third infringement: an uploading of the same song identified in the second notice. However, the Tribunal, in dismissing claims of unauthorised use, concluded it was "satisfied that file sharing took place via the respondent's internet account".[40] It then dismissed s 122O(5), only peripherally alluding to it.[41]

The Tribunal's conclusion does nothing to dispel the notion that a third party could have hacked into the account in order to commit the infringing act. It may have been prudent

[36] *RIANZ v Telecom NZ 2592* [2013] NZCOP 1 at [9]; *RIANZ v Telecom NZ 3663* [2013] NZCOP 7 at [5]; *RIANZ v Telecom NZ 2688* [2013] NZCOP 13 [36].
[37] [2013] NZCOP 1 [16]-[17]; [2013] NZCOP 7 at [8]; [2013] NZCOP 13 at [36].
[38] *RIANZ v Telecom NZ 2592* [2013] NZCOP 1 at [9].
[39] Ibid at [9].
[40] Ibid at [14].
[41] Ibid at [16]-[17].

for the Tribunal to make it clear that they were not accepting the respondent's excuse before dismissing s 122O(5). This would give future respondents a better idea of how to guard themselves against infringement notices consisting of unauthorised third party infringement and how to compile evidence in proof of this.

In [2013] NZCOP 7, The Tribunal considered the respondent's inference of unauthorised use "irrelevant to liability".[42] This conclusion is correct per s 122O(1)(a)(ii), which only requires that the infringement occurred at the account holders IP address. This would still occur in the case of Wi-Fi hacking. However, it is not irrelevant to manifest injustice. The Tribunal engaged in a tangential analysis of s 122(2) and s 122(3), in which it tentatively concluded the evidentiary presumptions stood.[43] However, this analysis only resolved that the file sharing occurred at the IP address of the account holder, which does nothing to dispel the presence of Wi-Fi hacking. Regardless, the Tribunal did "not consider that s 122O(5) applies" and neglected to undertake a significant manifestly unjust analysis.[44] Again, it may have been prudent for the Tribunal to determine the validity of the respondent's inference of Wi-Fi hacking before dismissing s 122O(5).

An evidentiary analysis of respondents' claims of unauthorised use would encounter numerous and insurmountable hurdles. The Tribunal will almost always lack the evidence to deduce whether Wi-Fi hacking occurred. Procuring the relevant evidence in proof of unauthorised access is beyond the technical capacity of the average respondent.

[42] *RIANZ v Telecom NZ 3663* [2013] NZCOP 7 at [16].
[43] See Part V of this paper.
[44] *RIANZ v Telecom NZ 3663* [2013] NZCOP 7 at [8].

Accepting unsubstantiated claims would open the floodgates to erroneous assertions. Furthermore, "manifestly" per s 122O(5) suggests an evidenced reason is required.

The evidentiary problems facing an average respondent in evidencing unauthorised use are illustrated in [2013] NZCOP 13. Here the Tribunal, unlike in [2013] NZCOP 1 and 7, undertook a thorough examination of the respondent's claim of unauthorised use. The Tribunal emphasised that there was no attempt to substantiate the evidence suggesting unauthorised use (that nobody was home when infringement occurred) and that no reason was provided as to why the respondent never installed a Wi-Fi password.[45]

The Tribunal also took into account the applicant's advice to the respondent to search for and delete file sharing software in the case of inadvertent infringement.[46] However, this advice occurred after liability was prima facie established through the issuing of the enforcement notice, therefore should not be considered relevant. Nevertheless, [2013] NZCOP 13 is a step in the right direction as it gives due credence to unauthorised use allegations and gives future respondents an indication of how to successfully satisfy s 122O(5) by evidencing claims of unauthorised use.

The decision in [2013] NZCOP 13 illustrates that proper attention is now being given to claims of unauthorised use. Empowering account holders to evidence such claims could be achieved with a simple amendment. The Act's regulations stipulate what information must be contained in infringement notices.[47] These could be amended to include

[45] *RIANZ v Telecom NZ 2688* [2013] NZCOP 13 at [36].
[46] *RIANZ v Telecom NZ 2688* [2013] NZCOP 13 at [35].
[47] Copyright (Infringing File Sharing) Regulations 2011, reg 5.

information on how to prevent and detect Wi-Fi hacking. This would both prevent unauthorised use and provide less knowledgeable account holders with the tools to substantiate genuine claims of Wi-Fi hacking.

Information on Wi-Fi security is contained in information provided by the Ministry of Economic Development (now the Ministry of Business, Innovation and Employment), a link to which is required in detection notices.[48] However, this information only relates to hacking prevention, and, as will be discussed shortly, has proven inaccessible to some account holders.

2 Technological incapacity and inadvertent infringement

Technological incapacity resulting in the ignorance of the default uploading function of file sharing software significantly increases the likelihood of inadvertent infringement. The allegations of unauthorised user infringements may be made due to ignorance of this uploading function. Opponents of the Act argued it is likely to punish such ignorance. [49] However, the intention of the Act was arguably to educate this ignorance. A technological divide between generations is clear. A study revealed youth orientated content is disproportionately reflected in P2P traffic.[50] In a family context, it seems unjust to require the less knowledgeable account holder (generally the parent) to police the technologically savvy end user (generally the child).

[48] Ibid reg 5(1)(e).
[49] InternetNZ "Here's why we don't like the new law" 3strikesnz <www.3strikes.net.nz>.
[50] Alexandre Mateus and Jon Peha "Quantifying Global Transfers of Copyright Content using BitTorrent" (6 September 2011) Social Science Research Network <www.ssrn.com> at 37.

It could be argued this knowledge disparity is relieved by information provided by the Ministry of Economic Development (MED), a link to which is required in detection notices.[51] This information explains how to prevent file sharing.[52] However, in practice this information has had little effect.

In [2013] NZCOP 2, the respondent argued he lacked the ability to prevent end user infringement. He highlighted the fact that he had very little computer literacy.[53] The Tribunal dispelled any notion of manifest unjustness by pointing to the fact that the respondent had the technical know-how to uninstall file sharing software after the third notice.[54] That the Tribunal found it necessary to prove some form of computer literacy on the part of the account holder suggests complete computer illiteracy may be grounds for finding manifest injustice.

In [2013] NZCOP 6, the respondent submission was as follows.[55] After the first detection notice the respondent warned their three young children. A second notice arrived, and the respondent singled out the child responsible and provided further warning. However, a third notice arrived, triggered by the uploading of the same song which gave rise to the second notice. They noted that they had then taken further action, with the help of a friend, by updating all passwords to ensure the children would not have internet access

[51] Copyright (Infringing File Sharing) Regulations 2011, reg 5(1)(e).
[52] Ministry of Economic Development "Notice Regime Under Sections 122A to U of the Copyright Act. How Does it Work?" Ministry of Business, Innovation and Employment <www.med.govt.nz> at 7.
[53] *RIANZ v TCLE[A]-T5877102* [2013] NZCOP 2 at [17].
[54] Ibid at [30].
[55] *RIANZ v Telecom NZ 3553* [2013] NZCOP 6 at [17].

without their supervision.[56] The Tribunal did not consider that a family situation wherein blame had been cast upon the children coupled with the parents' computer illiteracy gave rise to manifest injustice.[57]

In [2013] NZCOP 12, it transpired that the infringing activity was caused by a visitor who had been unwittingly uploading a song which had been downloaded two years earlier.[58] The respondent was technologically illiterate but took proactive steps to prevent the infringement and sought help from his ISP, which was not forthcoming until after the issue of the enforcement notice.[59] The Tribunal, when declining to engage s 122O(5), decided that respondent should have sought advice from other parties rather than the ISP.[60] It also considered that, since the applicant did not challenge the first two notices, the applicant could not have given advice regarding file sharing software.[61]

It is interesting to note that the Tribunal did not mention the information provided by the MED even though it is required to be linked to by infringement notices.[62] This contained all the advice necessary to identify the visitor's inadvertent uploading. Similarly, in [2013] NZCOP 7, the applicant was punished by a reduction of the penalty sum per s 122O(3)(a) for acknowledging that the infringement was likely caused through an automated

[56] Ibid at [18].
[57] *RIANZ v Telecom NZ 3553* [2013] NZCOP 6 at [20].
[58] *RIANZ v TCLEA-T6518151* [2013] NZCOP 12 at [18].
[59] Ibid at [18].
[60] Ibid at [29].
[61] Ibid at [21].
[62] Copyright (Infringing File Sharing) Regulations 2011, reg 5(1)(e).

uploading function of P2P software, and yet, they failed to inform the respondent of this or how to prevent it.[63] Again, the MED information went unacknowledged.

The Tribunal's unwillingness to engage s 122O(5) in relation to technical incapacity likely reflects the educative function of the Act. However, certain changes could be made to prevent these inadvertent infringements from advancing to the Tribunal. The MED information appears to be inaccessible to some account holders. It requires scrutiny of the infringement notice to obtain the link to the MED website, exploration of that website to locate the relevant document, and finally, discovering the relevant information within that document.

The regulations could be amended to provide this information appears on the infringement notices.[64] In particular, more detailed information regarding the default uploading function of file sharing software and information on how to locate and uninstall this software should be included. This would effectively reduce the injustice caused by forcing technologically illiterate account holders to police more knowledgeable users.

C Absence of account holder

In [2013] NZCOP 5 the respondent's submission to the Tribunal raised good reason for engaging s 122O(5).[65] The respondent had just returned from military deployment overseas and was unaware of any downloading which took place during his absence. He could not determine which of the eight people with access to his internet IP address

[63] *RIANZ v Telecom NZ 3663* [2013] NZCOP 7 at [32].
[64] see Copyright (Infringing File Sharing) Regulations 2011, reg 5.
[65] *RIANZ v CAL012-E000609* [2013] NZCOP 5 at [9].

committed the infringing act as many of his flatmates were now dispersed around New Zealand. He also expressed apprehension in partaking in the proceedings due to the difficult transition from military to civilian life. He did, however, acknowledge he was responsible for the actions committed under his IP address and indicated a willingness to co-operate with the Tribunal.

Surprisingly, the Tribunal did not even consider whether s 122O(5) was engaged. The judgement only gives the provision a passing mention, suggesting it did not consider it an issue.[66] The only indication it gives towards the respondent's arguable innocence is a comment that the level of infringement was "not at the serious end of the scale".[67]
This implies a very high standard is demanded when activating s 122O(5). The Tribunal referred to the first two notices as serving an "educative" function.[68] However, given his absence, the respondent lacked the capacity to police the use of his internet and admonish the end users when these first two infringement notices were sent. The educative role of the notices are completely void considering the position of the respondent.

Any deterrent effect relies on the end users (in this case the flatmates) relationship with the account holder. The respondent submitted he had "spoken to the pers [sic] who have access to my internet IP address".[69] However, any deterrent effect may be negated by an end user's apathy towards the consequences forced upon the account holder. Thus,

[66] Ibid at [16].
[67] Ibid at [25].
[68] *RIANZ v CAL012-E000609* [2013] NZCOP 5 at [25].
[69] Ibid at [5].

arguably, the only purpose the Act serves in this context is to punish an innocent account holder.

Rick Shera, an intellectual property lawyer specialising in internet law, concurred that it was open for the Tribunal to find manifest unjustness but conceded this would be difficult considering the respondent made no submission regarding injustice.[70] However s 122O(5) only requires the "circumstances of the case" to satisfy it that an award would be manifestly unjust. The Tribunal need not rely on submissions invoking the defence.

Furthermore, the respondent was likely ignorant of the manifestly unjust defence, considering the Act's regulations do not require infringement notices to inform the recipient of this defence, but only of their ability to challenge each notice.[71] Such a challenge may provide the papers which may inform the Tribunal's decision to invoke s 122O(5). However, of course, in the circumstances, the respondent had no capacity to challenge the notices.

The respondent's inability to challenges notices due to military deployment is arguably grounds for a finding of manifest unjustness. Considering the decision in [2013] NZCOP 5, as Shera states, it is now "hard to imagine any circumstance" in which manifest injustice will be found.[72] This case demonstrates the injustice which may be caused by imposing vicarious liability when coupled with a tentative approach to s 122O(5).

[70] Ibid.
[71] Copyright (Infringing File Sharing) Regulations 2011, reg 5.
[72] Rick Shera "Manifestly Unjust?" (13 March 2013) Law Geek NZ <www.lojo.co.nz>.

D Determination of award sum

The Tribunal's application of provisions regulating the determination of the penalty sum has eased the harshness of vicarious liability. If the Tribunal lacked this discretion, it is likely it would be compelled into a liberal reading of s 122O(5). The average fee awarded in proceedings thus far is $521.69.

Section 122O(3)(a) requires that the sum include a contribution to the cost incurred by the copyright owner when paying the ISP to issue an infringement notice (up to $25.00 per notice).[73] The Tribunal, in order to reflect the educative role of each notice, has adopted a sliding scale. The respondent is liable for one-third the cost of the detection notice, two-thirds the cost of the warning notice and the entire cost of the enforcement notice.[74] In [2013] NZCOP 7 the Tribunal avoided determining the validity of the respondent's inference of unauthorised, likely because of evidentiary difficulties.

Instead, the Tribunal lowered the sum by highlighting a separate issue. It censured the applicant for suggesting the infringement was likely caused through an automated uploading function yet it failed to inform the respondent of this or how to prevent it. The Tribunal subsequently lowered the sum per s 12O(3)(a) for failing to fulfill the educative function of the notices.[75] Perhaps this, along with evidentiary issues, explains the

[73] Copyright (Infringing File Sharing) Regulations 2011, reg 7.
[74] See *RIANZ v Telecom NZ 2592* [2013] NZCOP 1 at [26]; *RIANZ v TCLE[A]-T5877102 [2013]* NZCOP 2 at [64]; *RIANZ v CAL2013-E000614* [2013] NZCOP 3 at [28].
[75] *RIANZ v Telecom NZ 3663* [2013] NZCOP 7 at [32]

Tribunal's decision not to engage s 122O(5) and instead find another means to prescribe a "relatively modest award" of $276.78.[76]

Section 122O(2) requires that the sum be determined in accordance with the Act's regulations. The regulations stipulate the sum must include "an amount that the Tribunal considers appropriate as a deterrent against further infringing." The regulations guide the calculation of this amount by binding the Tribunal to consider the flagrancy of the infringement, the possible effect on the market for the infringed work, and whether the sum thus far would constitute a sufficient deterrent.[77]

The decision in [2013] NZCOP 7, in the face of unauthorised use allegations, saw the award of a relatively low deterrence fee of $50.00.[78] In [2013] NZCOP 6, the Tribunal considered the family setting coupled with the respondent's technological incapacity required only a deterrent fee of $60.00 with the total sum amounting to $316.97.[79] In [2013] NZCOP 6, where the respondent was completely absent, both Tribunal and applicant agreed to completely waive any deterrent sum and the respondent was charged the lowest fee to date, $255.97.[80] Similarly, in [2013] NZCOP 12, when the respondent was liable for a visitor's inadvertent downloading, the deterrent fee was completely waived, resulting in a fee of $276.63.[81]

[76] *RIANZ v Telecom NZ 3663* [2013] NZCOP 7 at [8].
[77] Copyright (Infringing File Sharing) Regulations 2011, reg 12(2)(d).
[78] *RIANZ v Telecom NZ 3663* [2013] NZCOP 7 at [42].
[79] *RIANZ v Telecom NZ 3553* [2013] NZCOP 6 at [46].
[80] *RIANZ v CAL012-E000609* [2013] NZCOP 5 at [10].
[81] *RIANZ v TCLEA-T6518151* [2013] NZCOP 12 at [23].

This lack of need for deterrence can be construed as a reflection of lack of guilt on the account holder's part. In neglecting to find manifest injustice, The Tribunal, has turned to the deterrence fee as a means of recognising lack of guilt. If this discretion was not available, for example a fixed deterrent fee for each infringement was stipulated, it is more likely that s 122O(5) would be invoked. However, the fees guiding penalty sum determination allow the Tribunal to cast its eyes elsewhere, and, as in some cases, avoid a s 122O(5) inquiry altogether.

E Flagrancy of infringement

A similar fee limiting approach could be adopted in regard to the flagrancy consideration in determination of a deterrent sum per reg 12(3)(a). This would directly address the vicarious liability component of the Act. As delineated in [2013] NZCOP 14, 'flagrancy' is considered in the narrow context of the deterrence sum rather than, as in the Copyright Act 1994, in the light of what justice requires.[82] The Tribunal has stated that "flagrancy suggests something beyond the normal case".[83] The Tribunal has dismissed judicial precedent regarding the meaning of 'flagrancy' due to the quasi-judicial nature of the Tribunal.[84] Therefore, it is open for the Tribunal to define this extra element required for flagrancy in the context of a sum deterring future infringing.

A 'normal case' under the Act can be described as finding an incidence of file sharing resulting in an infringement which occurred at the IP address of the account holder. This

[82] *RIANZ v Telecom NZ 3760* [2013] NZCOP 14 at [36].
[83] Ibid at [37].
[84] *RIANZ v CAL2013-E000614* [2013] NZCOP 3 at [34].

incidence may be brought about by either the account holder or an end user, intentionally or otherwise. Where an account holder *intentionally* brings about this incidence *him or herself*, this could be described as 'beyond the normal case' as thus may qualify as flagrant.

This would have the effect of creating a division between account holders intentionally infringing and those who those who did not. This dichotomy would reduce the harshness of the vicarious liability component by increasing deterrence for account holders intentionally infringing, and, by contrast, prescribing a lighter penalty for those who were unaware of end user infringement. This is within the flagrancy realm of deterrence, as intentional account holders require further deterrence as compared to unintentional account holders.

One half of this proposed approach was, by inference, supported by the applicant's submissions in [2013] NZCOP 7. The respondent claimed they were at work during the time of the infringement giving rise to the detection notice.[85] The applicants stated in response that they did not contend the infringement was flagrant.[86] This can be attributed to their acceptance of the respondent's submission that they were at work during the infringement, thus could not have committed it themselves. The Tribunal viewed this "appropriate concession".[87] Therefore, both the Tribunal and the applicant have viewed it as appropriate to dismiss flagrancy contentions where it is shown that the account holder themselves did not partake in the infringing activity.

[85] *RIANZ v Telecom NZ 3663* [2013] NZCOP 7 at [5].
[86] Ibid at [6].
[87] Ibid at [38]

This approach may lead to respondents automatically denying involvement in infringement, but as [2013] NZCOP 1 illustrates, it is possible for respondents to admit intentional infringing.[88]

IV The Evidentiary Presumptions

A Reading section 122N(1) as imposing strict liability

Section 122O(1) stipulates that where three factors are present an award must be made:

1. That each of the three alleged infringements triggering the infringement notice constituted an infringement of the rights of the copyright owner;[89]
2. That said infringements occurred at the IP address of the account holder; and [90]
3. That the three notices were issued in accordance with this Act.[91]

The three evidentiary presumptions within s 122N(1) align with these required factors:

1. Each incidence of file sharing identified in the infringement notices constituted an infringement; [92]
    - This presumption satisfies factor one, as the two provisions are tantamount.
2. That the information recorded in this notice is correct; and [93]

[88] *RIANZ v Telecom NZ 2592* [2013] NZCOP 1 at [9].
[89] Copyright (Infringing File Sharing) Amendment Act 2011, s 122O(1)(a)(i).
[90] Ibid, s 122O(1)(a)(ii).
[91] Ibid, s 122O(1)(b).
[92] Ibid, s 122N(1)(a).
[93] Ibid, s 122N(1)(b).

- This presumption satisfies factor two, as the infringement notices must identify the account holders IP address.[94]

3. That each infringement notice was issued in accordance with this Act.[95]
    - This presumption satisfies factor three, as the two provisions are tantamount.

This demonstrates where the presumptions apply liability is automatically established. Section 122N(2) provides this presumption may be rebutted, but, s 122N(3) provides that the rebuttal itself may be negated. Therefore whether s 122N could be veritably described as imposing strict liability depends upon the threshold required to engage ss 122N(2) and 122N(3).

B Policy rationale for evidentiary presumptions

These presumptions address the problem of the evidentiary veil provided by private home internet use. It expedites the process by avoiding complex disputes regarding detection software. However, two issues raise concern.

The first is the potential for erroneous detections. The RIANZ employs MarkMonitor when detecting infringements.[96] This service identifies infringing IP addresses and provides "extensive forensic evidence".[97] The legislature has placed faith in such services as the evidentiary presumptions effectively presume detections by MarkMonitor constitute an incidence of infringing file sharing. An 'independent' assessment of MarkMonitor's

[94] Copyright (Infringing File Sharing) Amendment Regulations 2011, regs 4(2)(a) and cl 5(1)(a).
[95] Copyright (Infringing File Sharing) Amendment Act 2011, s 122N(1)(b).
[96] *RIANZ v TCLE[A]-T5877102* [2013] NZCOP 2 at [21].
[97] "Services: Anti-Piracy" MarkMonitor <markmonitor.com>.

methodology has found it robust, accurate and capable of withstanding scrutiny or evidentiary challenges.[98] However, the conductor of this assessment was a former paid lobbyist for the Recording Industry Association of America (the parent association of RIANZ), and erroneous detections by MarkMonitor have been reported.[99] Therefore, erroneous detections may possibly form the basis for infringement notices.

Another issue is the possibility of altogether bogus claims. In a document referred to the Select Committee, Google Incorporated highlighted that of the notices it received under the Digital Millennium Copyright Act 1998 (US), 37% were not valid copyright claims.[100] Justice David Harvey, in a similar submission, stated that "some 30%" of copyright litigation fails on the grounds that the copyright owner does not hold the copyright and that such copyright is not governed by New Zealand law.[101]

Section 122N(2) possibly remedies these issues by allowing an account holder to challenge the presumptions in the event of erroneous detection and bogus claims. However, the account holder, generally a single layperson, will often lack the technical capacity for such an exercise. For example, one respondent displayed "computer illiteracy".[102] Considering the resource asymmetry between a copyright holder, a well-funded association of global companies, and the typical account holder, there is a good argument to remove this presumption. Entities like RIANZ are in the better position to prove an actual infringement

[98] Stroz Friedberg "Independent Expert Assessment of MarkMonitor AntiPiracy Methodologies" (1 November 2012) Center for Copyright Information <www.copyrightinformation.org> at 3.
[99] "False MarkMonitor flags raises more 'six strikes' concerns" *Electronista* (online ed, 6 March 2013).
[100] Google Incorporated "Internet Service Provider Code of Practice – TCF Consultation Draft" (6 March 2009) New Zealand Telecommunications Forum <www.tcf.org.nz> at 9.
[101] David Harvey, "Submission to the Telecommunications Carriers Forum" (27 February 2009) New Zealand Telecommunications Forum <www.tcf.org.nz> at 2.
[102] *RIANZ v Telecom NZ 3553* [2013] NZCOP 6 at [20].

occurred through validating detection software, rather for the account holder to disprove the infringement occurred.

Regardless, the onus is on the account holder to reverse the evidentiary presumption. This task has proven exceedingly difficult.

V Rebutting the Evidentiary Presumptions

Section 122N(2) allows an account holder to "submit evidence that, or give reasons why" any of the evidentiary presumptions should not apply. Where such submissions are made, s 122N(3) provides that the onus springs back to the copyright owner who must then "satisfy the Tribunal that" the presumptions are correct. [2013] NZCOP 7 and 9 involved detailed discussions of ss 122N(2) and 122N(3).

A The standard required to engage section 122N(2)

It could be argued that bare claims are enough to engage s 122N(2). In [2013] NZCOP 7 the Tribunal undertook a tangential discussion of the interplay between ss 122N(2) and 122N(3) in the context of first two evidentiary presumptions. The respondents submitted to the Tribunal that the infringed work was not on any household computers, inferring unauthorised use occurred.[103] The applicant replied by noting that "the account holder did not provide evidence or independent verification" to evidence this claim. [104]

[103] *RIANZ v Telecom NZ 3663* [2013] NZCOP 7 at [5] and [6].
[104] Ibid at [17].

As discussed, an inference of unauthorised use is "irrelevant to liability" as the Act "makes the *account holder* liable".[105] The Tribunal, supposing hypothetically that this inference of unauthorised use could engage s 122(2), censured the applicant's response, as it "belied" s 122N(3) by assuming that the onus to rebut the evidentiary presumption remained with the respondent, even after engaging s 122N(2).[106] This hypothetical analysis indicates that *unsubstantiated* claims have the potential to engage s 122N(2).

In [2013] NZCOP 9, the respondent alleged that they had not received any infringement notices from their Internet provider, only their monthly bill.[107] Although the Tribunal did not explicitly allude to engagement of s 122N(2), it considered this submission raised an issue over the third presumption contained in s 122(N)(1)(c); that the infringement notice was issued in accordance with this Act. [108] It could be inferred that the Tribunal believed this bare allegation engaged s 122N(2) by constituting a "reason why" the presumption should not apply. This is supported by the Tribunal's subsequent interpretation of the applicant's response to this allegation, which may be construed as the applicant's attempt to "satisfy" the court that the s 122N(1)(c) presumption was correct per s 122N(3).[109] A contrary interpretation will be discussed later.

This low standard is supported by a close reading of s 122N(2) which allows the user to submit "evidence that, *or* give reasons why" the presumption does not apply (emphasis added). This suggests Parliament acknowledged a dichotomy between bare claims and

[105] Ibid at [16].
[106] Ibid at [18].
[107] *RIANZ v CAL2012-E000627* [2013] NZCOP 9 at [19].
[108] Ibid at [26].
[109] Ibid at [28] to [32].

those supported by evidence, and chose to allow both. Section 122N(2)'s proto-provision within the Copyright (Infringing File Sharing) Amendment Bill read: [110]

> "An account holder may submit evidence, or give reasons, *that show* that any 1 or more of the presumptions in subsection (1) do not apply with respect to any particular infringement identified in an infringement notice." (emphasis added)

The word "show", which has been omitted from s 122N(2), conveys a higher threshold by indicating that the Tribunal must be convinced that the presumptions do not apply. Its removal suggests that Parliament acknowledged that the standard within the Bill was in appropriately high. Without "show", the Tribunal need not be convinced of anything, it only requires for submissions to provide evidence that or reasons why the presumption should not apply. Once these are provided, s 122N(2) is engaged.

From a policy perspective, it would make sense to require a higher standard of proof - that is sound evidence, when engaging s 122N(2). Shera argued that if an unsubstantiated claim were able to rebut the evidentiary presumption, for example "it wasn't me", then this would "render the presumption no presumption at all".[111] Indeed, if unsubstantiated claims were accepted, it could open the floodgates whereby every single respondent would submit bare denials of infringing incidents. Although s 122N(3) would stem the flow caused by this potential torrent.

---

[110] Copyright (Infringing File Sharing) Amendment Bill 2010 (119-2), cl 12MA(2).

[111] Rick Shera "Groundhog Day: Guilty Until Proven Innocent" (10 November 2010) Institute of IT Professionals New Zealand <www.iitp.org.nz>.

Countervailing policy considerations support a low standard. Section 122N(2) may operate as a check on bogus claims or those based on erroneous detection. In order to combat such claims, account holders with a firm belief that no infringement took place at their IP address may raise this point without further evidence. The problem of evidencing such a belief is resolved by a low standard of proof. However, this check could be nullified depending on the standard required to engage s 122N(3).

B The standard required to engage section 122N(3)

In [2013] NZCOP 9 the applicants, in reaction to the respondent's allegation that no infringement notices had been received, provided information from the ISP verifying notices had been sent to the physical and email address of the respondent.[112] The Tribunal's evaluation was twofold. Firstly, it emphasised since the respondent had received, via physical address, the formal notice informing them of the present proceedings, there was no reason to believe the respondent's allegation.[113] This alone could be enough to deduce the respondent's allegation was spurious thus satisfying s 122N(3).

Secondly, the Tribunal highlighted the respondent's failure to challenge the evidence provided by the ISP. [114] It also considered that no explanation as to why the infringement notices would not have reached her billing address had been offered.[115] It could be argued that these second considerations were ultra vires. They may be subject to the same

[112] *RIANZ v CAL2012-E000627* [2013] NZCOP 9 at [28].
[113] Ibid at [29] and [30].
[114] Ibid at [31].
[115] Ibid.

tangential criticism which the Tribunal in [2013] NZCOP 7 levelled at the applicant's reply to the respondent's submission.[116] That is that they belie s 122N(3), by assuming the onus is still on the respondent to rebut the presumptions, even after s 122N(2) is engaged. The onus, after engagement of s 122N(2), rests solely upon the account holder. Any contemplation of the respondent's failure to critique the evidence provided by the ISP in the applicant's reply is immaterial.

However, as the Tribunal in [2013] NZCOP 9 makes no explicit reference to ss 122N(2) or 122N(3), it could be argued that the second class of considerations were relevant to the initial s 122N(2) rebuttal. That is, the respondent's failure to critique the ISP evidence and provide evidence meant the claim towards s 122N(2) was unsubstantiated and thus void. This analysis should not be preferred as it contradicts the low standard which, as established above, should be required to engage s 122N(2).

In [2013] NZCOP 7, the Tribunal, in its mock assessment of s 122(2) and s 122(3), considered the applicant's submission which detailed the reliability of the detection methods.[117] Assuming that s 122N(2) was engaged, then this would have 'satisfied' the Tribunal that the presumptions were correct per s 122N(3).[118] However, the Tribunal highlighted that "satisfy" per s 122N(3) was a high threshold.[119] It noted that the information provided regarding the evidence gathering method was thin and a fuller

[116] *RIANZ v Telecom NZ 3663* [2013] NZCOP 7 at [18].
[117] *RIANZ v Telecom NZ 3663* [2013] NZCOP 7 at [18].
[118] Ibid at [18].
[119] Ibid at [18].

explanation would be "preferable".[120] It also considered that other factual circumstances may "provoke a more testing exposition of these issues."[121]

Such factual circumstances may include where a respondent produces substantiated "evidence that" the presumptions should not apply per s 122N(2). Although, as established, evidence should not be required to engage s 122N(2) - an evidenced defence would demand a much higher standard of response in the form of s 122N(3).

C Case for removing presumptions

Where a bare claim engages s 122N(2), it is likely that a low standard is required to satisfy s 122N(3). This may be justified on the grounds that it protects the presumptions from being defeated by spurious challenges by respondents. However, it may also lead to upholding the presumptions in the face of genuine cases of erroneous detection or bogus claims. Respondents will rarely have the means or ability to put up anything beyond a bare claim. As a result, in the majority of cases, s 122N(2) will only be engaged by a bare claim and the respondent only needs to provide a detailed description outlining the reliability of their detection method. Consequently, almost invariably, the evidentiary presumptions of s 122N(1) will operate in conjunction with s 122O(1) and impose a strict form of liability. In other words, if a copyright owner detects three infringements on an account holder's account this will lead to an award being granted.

[120] Ibid at [18].
[121] Ibid at [18].

The evidentiary presumptions could be justifiably removed. This would require that in each case the applicant would have to prove an infringement occurred at the respondent's IP address and that the notices were issued in accordance with the Act. This would reduce the expediency of the regime by restoring the evidentiary hurdles present prior to the Act. However, applicants (to date, exclusively RIANZ) possess the resources to overcome these hurdles and, conversely, respondents are ill-equipped to rebut evidentiary presumptions. Furthermore, expediency should not come at the risk of injustice posed erroneous detection and false claims. To prove that infringement occurred, respondents could detail their detection techniques. The Tribunal would have to assess whether these techniques were reliable. An independent Parliamentary assessment as to the reliability of the detection services employed by RIANZ could remove this burden from the Tribunal.

VI Conclusion

File sharing software, like other historical developments in dissemination technology, has provoked the legislature into action. The Act represents an ambitious but ultimately flawed attempt to overcome the authorisation, detection and evidentiary hurdles involved in taking enforcement action against infringing file sharing.

The decision to hold account holders vicariously liable for end user infringements eschews the evidentiary and authorisation hurdles allowing for a workable regime. However, in doing so, it gives rise to the potential for injustice. From a policy perspective, a clear assumption of responsibility should be found before imposing vicarious liability. An

advertisement campaign educating account holders as to these responsibilities would remedy this. Further steps could be taken to address certain fact patterns that have arisen in the Tribunal. The Act should contain discretion to charge end users where they admit to infringing activities. The information contained in infringement notices should contain information regarding prevention and detection of Wi-Fi hacking, so that account holders might be able to evidence claims indicating manifest unjustness. Similarly, these notices should hold detailed information about the uploading function of file sharing software and how to uninstall it. This would reduce the potential for inadvertent infringement. Finally, a fee limiting approaching could be adopted in the context of flagrancy in in order to establish a dichotomy between account holders directly infringing and those vicariously liable.

The s 122N(1) presumptions pierce the evidentiary veil provided by file sharing. However, this comes at the cost of validating claims based on erroneous detections or altogether bogus claims. Section 122N(2) potentially assuages this risk. However, in reality respondents will only be able to muster bare claims towards s 122N(2). If accepted, these bare claims will likely be easily negated by applicant submissions under s 122N(3). The removal of the evidentiary presumptions could be justified based on the grounds of resource asymmetry between applicants and respondents. This would ensure an appropriate balance between expediency and justice.

VII Bibliography

A Legislation

1 New Zealand

Copyright (Infringing File Sharing) Amendment Act 2011.

Copyright (Infringing File Sharing) Regulations 2011.

Land Transport Act 1998.

2 United Kingdom

Licensing of the Press Act 1662 (UK) 14 Car c 33.

The Statute of Anne 1710 (UK) 8 Anne c 33.

B Cases

1 Australia

Roadshow Films v iiNet [2012] HCA 16.

2 New Zealand

RIANZ v CAL012-E000609 [2013] NZCOP 5.

RIANZ v CAL2012-E000627 [2013] NZCOP 9.

RIANZ v CAL2013-E000614 [2013] NZCOP 3.

RIANZ v TCLE[A]-T5877102 [2013] NZCOP 2.

RIANZ v TCLEA-T6518151 [2013] NZCOP 12.

RIANZ v Telecom NZ 2592 [2013] NZCOP 1.

RIANZ v Telecom NZ 2688 [2013] NZCOP 13.

RIANZ v Telecom NZ 3553 [2013] NZCOP 6.

RIANZ v Telecom NZ 3663 [2013] NZCOP 7.

RIANZ v Telecom NZ 3728 [2013] NZCOP 8.

RIANZ v Telecom NZ 3760 [2013] NZCOP 14.

C Journal Articles

Raymond Astbury "The Renewal of the Licensing Act in 1693 and its Lapse in 1695" (1978) s5-XXXIII Library 296.

Thomas Morris "The Origins of the Statute of Anne" (1962) 12 Copyright L Symp (ASCAP) 222.

D Official Sources

Hansard 22 April 2010 Volume 662 Week 39: Copy Copyright (Infringing File Sharing) Amendment Act 2011 First Reading.

Hansard 12 April 2011 volume 671 week 71: Copyright (Infringing File Sharing) Amendment Act 2011 Second Reading.

E Online Sources

Encyclopaedia Britannica <www.britannica.com>.

Alexandre Mateus and Jon Peha “Quantifying Global Transfers of Copyright Content using BitTorrent” (6 September 2011) Social Science Research Network <www.ssrn.com>.

Kartikey Mahajan “Corporate Criminal Liability: Why Corporations are Preferred and Not the Employees?” (6 May 2010) Social Science Research Network <www.ssrn.com>.

InternetNZ 3strikesnz <www.strikes.net.nz>.

“Telecom broadband terms and conditions” <www.telecom.co.nz>.

“Orcon Terms and Conditions” <www.orcon.net.nz>.

Ministry of Business, Innovation and Employment <www.med.govt.nz>.

Rick Shera Law Geek NZ <www.lojo.co.nz>.

New Zealand Telecommunications Forum <www.tcf.org.nz>.

Electronista (online ed) < Electronista.com >.

“Services: Anti-Piracy” MarkMonitor <markmonitor.com>.

Center for Copyright Information <www.copyrightinformation.org>.

New Zealand Listener (online ed) < www.listener.co.nz>.

Word Count (excluding title page, table of contents, bibliography and footnotes): 7995