FEDERAL COURT OF AUSTRALIA

Roadshow Films Pty Ltd v iiNet Limited (No. 3) [2010] FCA 24

SUMMARY

Citation:	Roadshow Films Pty Ltd v iiNet Limited (No. 3) [2010] FCA 24
Parties:	**Roadshow Films Pty Ltd (ACN 100 746 870) and the parties in the attached Schedule I v iiNet Limited (ACN 068 628 937)**
File number:	NSD 1802 of 2008
Judge:	**COWDROY J**
Date of judgment:	4 February 2010

Roadshow Films Pty Ltd v iiNet Limited (No. 3) [2010] FCA 24

SUMMARY

1 **In accordance with the practice of the Federal Court in some cases of public interest, importance or complexity, the following summary has been prepared to accompany the orders made today. This summary is intended to assist in understanding the outcome of this proceeding and is not a complete statement of the conclusions reached by the Court. The only authoritative statement of the Court's reasons is that contained in the published reasons for judgment which will be available on the internet at www.fedcourt.gov.au.**

2 The judgment in this proceeding is necessarily complicated both as to fact and law. It is also lengthy, running for 636 paragraphs and almost 200 pages. I have decided to provide short oral reasons for the judgment which I am presently to hand down. These reasons are not intended to be a substitute for reading the judgment itself which will be accessible online this morning.

3 This proceeding raises the question whether an internet service provider or ISP authorises the infringement of copyright of its users or subscribers when they download cinematograph films in a manner which infringes copyright. In Australian copyright law, a person who authorises the infringement of copyright is treated as if they themselves infringed copyright directly.

4 This proceeding has attracted widespread interest both here in Australia and abroad, and both within the legal community and the general public. So much so that I understand this is the first Australian trial to be twittered or tweeted. I granted approval for this to occur in view of the public interest in the proceeding, and it seems rather fitting for a copyright trial involving the internet.

5 That this trial should have attracted such attention is unsurprising, given the subject matter. As far as I am aware, this trial, involving suit against an ISP claiming copyright infringement on its part due to alleged authorisation of the copyright infringement of its users or subscribers, is the first trial of its kind in the world to proceed to hearing and judgment.

6 The 34 applicants who have instituted this claim represent the major motion picture studios both in Australia and the United States. They have brought this proceeding against iiNet which is the third largest ISP in Australia. An organisation known as the Australian Federation Against Copyright Theft or AFACT has, on behalf of the applicants, been prominent in the conduct of the claim.

7 AFACT employed a company known as DtecNet to investigate copyright infringement occurring by means of a peer to peer system known as the BitTorrent protocol by subscribers and users of iiNet's services. The information generated from these investigations was then sent to iiNet by AFACT, with a demand that iiNet take action to stop the infringements occurring. The measures which AFACT requested iiNet perform were never precisely elucidated. However, as the evidence at trial indicated, AFACT wanted iiNet to send a warning to the subscriber who was allegedly infringing. If a warning was not sufficient to stop the infringement, AFACT intended that iiNet suspend the internet service of that subscriber. If the subscriber remained unco-operative, termination of the internet service was sought as the ultimate sanction. In addition, or in the alternative, the applicants suggested that iiNet should block certain websites.

8 The evidence of infringement gathered by AFACT utilised the BitTorrent protocol, a blueprint for a highly efficient and effective mechanism to distribute large quantities of data. This protocol was created in 2001. It has been used, or more accurately, the constituent parts of the protocol (such as the client, tracker and .torrent files) have been used by those accessing the internet through iiNet's facilities (the 'iiNet users') to download the applicants' films and television shows in a manner which infringes copyright. I shall refer to the constituent parts of the BitTorrent protocol together as the BitTorrent system.

9 The critical issue in this proceeding was whether iiNet, by failing to take any steps to stop infringing conduct, authorised the copyright infringement of certain iiNet users.

10 The first step in making a finding of authorisation was to determine whether certain iiNet users infringed copyright. I have found that they have. However, in reaching that finding, I have found that the number of infringements that have occurred are significantly fewer than the number alleged by the applicants. This follows from my finding that, on the evidence and on a proper interpretation of the law, a person makes each film available online only once through the BitTorrent system and electronically transmits each film only once

through that system. This excludes the possible case of a person who might repeatedly download the same file, but no evidence was presented of such unusual and unlikely circumstance. Further, I have found, on the evidence before me, that the iiNet users have made one copy of each film and have not made further copies onto physical media such as DVDs.

11 The next question was whether iiNet authorised those infringements. While I find that iiNet had knowledge of infringements occurring, and did not act to stop them, such findings do not necessitate a finding of authorisation. I find that iiNet did not authorise the infringements of copyright of the iiNet users. I have reached that conclusion for three primary reasons which I now refer to.

12 Firstly, in the law of authorisation, there is a distinction to be drawn between the provision of the 'means' of infringement compared to the provision of a precondition to infringement occurring. The decisions in *Moorhouse, Jain, Metro, Cooper* and *Kazaa* are each examples of cases in which the authorisers provided the 'means' of infringement. But, unlike those decisions, I find that the mere provision of access to the internet is not the 'means' of infringement. There does not appear to be any way to infringe the applicants' copyright from the mere use of the internet. Rather, the 'means' by which the applicants' copyright is infringed is an iiNet user's use of the constituent parts of the BitTorrent system. iiNet has no control over the BitTorrent system and is not responsible for the operation of the BitTorrent system.

13 Secondly, I find that a scheme for notification, suspension and termination of customer accounts is not, in this instance, a relevant power to prevent copyright infringement pursuant to s 101(1A)(a) of the *Copyright Act*, nor in the circumstances of this case is it a reasonable step pursuant to s 101(1A)(c) of the *Copyright Act*. The reason for this finding is complicated and lengthy, and is not suitable for reduction to a short summary for present purposes so I shall refrain from attempting to do so.

14 Thirdly, I find that iiNet simply cannot be seen as sanctioning, approving or countenancing copyright infringement. The requisite element of favouring infringement on the evidence simply does not exist. The evidence establishes that iiNet has done no more than to provide an internet service to its users. This can be clearly contrasted with the respondents in the *Cooper* and *Kazaa* proceedings, in which the respondents intended copyright

infringements to occur, and in circumstances where the website and software respectively were deliberately structured to achieve this result.

15 Consequently, I find that the applicants' Amended Application before me must fail. However, for the sake of completeness, I have considered all the issues argued before me.

16 I find that the *Telecommunications Act* would not have operated to prohibit iiNet from acting on the AFACT Notices of infringement. However, as I have already found that iiNet did not authorise copyright infringement, such issue is irrelevant.

17 I find that s 112E of the *Copyright Act* would not have operated to prevent a finding of authorisation of copyright infringement against iiNet. However, as I found on conventional principles of authorisation that the respondent did not authorise copyright infringement, such issue is irrelevant.

18 Finally, I find that iiNet did have a repeat infringer policy which was reasonably implemented and that iiNet would therefore have been entitled to take advantage of the safe harbour provisions in Division 2AA of Part V of the *Copyright Act* if it needed to do so. I have drawn assistance from United States authority dealing with similar statutory instruments in making the finding. While iiNet did not have a policy of the kind that the applicants believed was required, it does not follow that iiNet did not have a policy which complied with the safe harbour provisions. However, as I have not found that iiNet authorised copyright infringement, there is no need for iiNet to take advantage of the protection provided by such provisions.

19 The result of this proceeding will disappoint the applicants. The evidence establishes that copyright infringement of the applicants' films is occurring on a large scale, and I infer that such infringements are occurring worldwide. However, such fact does not necessitate or compel, and can never necessitate or compel, a finding of authorisation, merely because it is felt that 'something must be done' to stop the infringements. An ISP such as iiNet provides a legitimate communication facility which is neither intended nor designed to infringe copyright. It is only by means of the application of the BitTorrent system that copyright infringements are enabled, although it must be recognised that the BitTorrent system can be used for legitimate purposes as well. iiNet is not responsible if an iiNet user chooses to make use of that system to bring about copyright infringement.

20 The law recognises no positive obligation on any person to protect the copyright of another. The law only recognises a prohibition on the doing of copyright acts without the licence of the copyright owner or exclusive licensee, or the authorisation of those acts. In the circumstances outlined above and discussed in greater detail in my judgment, it is impossible to conclude that iiNet has authorised copyright infringement.

21 In summary, in this proceeding, the key question is: Did iiNet authorise copyright infringement? The Court answers such question in the negative for three reasons: first because the copyright infringements occurred directly as a result of the use of the BitTorrent system, not the use of the internet, and the respondent did not create and does not control the BitTorrent system; second because the respondent did not have a relevant power to prevent those infringements occurring; and third because the respondent did not sanction, approve or countenance copyright infringement.

22 I will now make my formal orders. For the reasons provided in the written judgment I make the following orders.

1. The Amended Application be dismissed.

2. Subject to Order 3 and 4, the Applicants pay the costs of the Respondent, including costs thrown away as a result of the Applicants' abandoning the primary infringement claim against the Respondent.

3. Any party or person applying for an order for costs different to that provided by Order 2 is to notify the Court within 14 days in which event Order 2 will be vacated and in lieu costs will be reserved.

4. If any application for costs is made as provided in Order 3 the parties and/or persons are to consult and prepare consent directions for the filing of submissions and, if required, for a hearing on costs.

23 I publish my reasons.

Cowdroy J

Sydney

4 February 2010

SCHEDULE I – THE APPLICANTS

UNIVERSAL CITY STUDIOS LLLP
Second Applicant

PARAMOUNT PICTURES CORPORATION
Third Applicant

WARNER BROS. ENTERTAINMENT INC.
Fourth Applicant

DISNEY ENTERPRISES, INC.
Fifth Applicant

COLUMBIA PICTURES INDUSTRIES, INC
Sixth Applicant

TWENTIETH CENTURY FOX FILM CORPORATION
Seventh Applicant

PARAMOUNT HOME ENTERTAINMENT (AUSTRALASIA) PTY LTD
Eighth Applicant

BUENA VISTA HOME ENTERTAINMENT, INC.
Ninth Applicant

TWENTIETH CENTURY FOX FILM CORPORATION (AUSTRALIA) PTY LIMITED
Tenth Applicant

UNIVERSAL PICTURES (AUSTRALIA) PTY LTD
Eleventh Applicant

VILLAGE ROADSHOW FILMS (BVI) LTD
Twelfth Applicant

UNIVERSAL PICTURES INTERNATIONAL B.V
Thirteenth Applicant

UNIVERSAL CITY STUDIOS PRODUCTIONS LLLP
Fourteenth Applicant

RINGERIKE GMBH & CO KG
Fifteenth Applicant

INTERNATIONALE FILMPRODUKTION BLACKBIRD VIERTE GMBH & CO KG
Sixteenth Applicant

MDBF ZWEITE FILMGESELLSCHAFT MBH & CO KG
Seventeenth Applicant

INTERNATIONALE FILMPRODUCKTION RICHTER GMBH & CO KG
Eighteenth Applicant

NBC STUDIOS, INC
Nineteenth Applicant

DREAMWORKS FILMS L.L.C
Twentieth Applicant

WARNER BROS INTERNATIONAL TELEVISION DISTRIBUTION INC
Twenty-First Applicant

TWENTIETH CENTURY FOX HOME ENTERTAINMENT INTERNATIONAL CORPORATION
Twenty-Second Applicant

WARNER HOME VIDEO PTY LTD
Twenty-Third Applicant

PATALEX III PRODUCTIONS LIMITED
Twenty-Fourth Applicant

LONELY FILM PRODUCTIONS GMBH & CO KG
Twenty-Fifth Applicant

SONY PICTURES ANIMATION INC
Twenty-Sixth Applicant

UNIVERSAL STUDIOS INTERNATIONAL B.V.
Twenty-Seventh Applicant

SONY PICTURES HOME ENTERTAINMENT PTY LTD
Twenty-Eighth Applicant

GH ONE LLC
Twenty-Ninth Applicant

GH THREE LLC
Thirtieth Applicant

BEVERLY BLVD LLC
Thirty-First Applicant

WARNER BROS ENTERTAINMENT AUSTRALIA PTY LTD
Thirty-Second Applicant

TWENTIETH CENTURY FOX HOME ENTERTAINMENT LLC
Thirty-Third Applicant

SEVEN NETWORK (OPERATIONS) LTD
Thirty-Fourth Applicant

FEDERAL COURT OF AUSTRALIA

Roadshow Films Pty Ltd v iiNet Limited (No. 3) [2010] FCA 24

Citation:	Roadshow Films Pty Ltd v iiNet Limited (No. 3) [2010] FCA 24
Parties:	**Roadshow Films Pty Ltd (ACN 100 746 870) and the parties in attached Schedule I v iiNet Limited (ACN 068 628 937)**
File number:	NSD 1802 of 2008
Judge:	**COWDROY J**
Date of judgment:	4 February 2010
Catchwords:	**INTELLECTUAL PROPERTY** – Copyright Authorisation – Internet Service Provider provided internet to subscribers – allegations made to Internet Service Provider that those using its internet service were infringing copyright – whether persons using the internet service of the respondent infringed copyright by making available online, electronically transmitting and making copies of applicants' films – whether the respondent authorised the infringement which occurred – whether the respondent provided the means of infringement – whether the respondent had the power to prevent the infringements which occurred – whether the respondent sanctioned, approved, countenanced the infringements which occurred – whether s 276 of the *Telecommunications Act 1997* (Cth) led to a finding that the respondent did not have the power to prevent infringement **INTELLECTUAL PROPERTY** – Copyright Authorisation – whether s 112E of the *Copyright Act 1968* (Cth) prevented the respondent from being found to have authorised – whether the respondent had knowledge of the infringements which occurred **INTELLECTUAL PROPERTY** – 'Safe Harbour' Provisions – whether the respondent complied with the provisions of Division 2AA of Part V of the *Copyright Act 1968* (Cth) – what constitutes a repeat infringer policy – whether respondent had a repeat infringer policy – whether respondent had implemented repeat infringer policy
Legislation:	*Broadcasting Services Act 1992* (Cth) *Copyright Act 1968* (Cth) ss 10, 14, 22(6), 22(6A), 37, 86,

100A, 101, 101(1A), 104, 112E, 115, 116AA, 116AC, 116AD, 116AE, 116AF, 116AG, 116AH(1), 116AH(2), 116AI, 119(a), 135ZWA
Copyright Amendment (Digital Agenda) Act 2000 (Cth)
Copyright Amendment (Digital Agenda) Bill 1999 (Cth)
Copyright Amendment Regulations 2004 (No. 1) (Cth)
Copyright, Designs and Patent Act 1988 (UK) s 45(1)
Copyright Legislation Amendment Act 2004 (Cth)
Copyright Regulations 1969 (Cth) reg 20B, 20I, 20J, 20K, 20L, 20M, 20X
Criminal Code 1995 (Cth) s 137.2
Digital Millennium Copyright Act 1998 (US) s 202
Telecommunications Act 1997 (Cth) ss 7, 87, 270, 276, 279, 280, 289, 290
Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth) s 128(5)
Telecommunications (Interception and Access) Act 1979 (Cth)
United States Code (US) Title 17 s 512
US Free Trade Implementation Act 2004 (Cth)

Cases cited:

Apand Pty Limited v The Kettle Chip Company Pty Limited (1994) 62 FCR 474 followed
Australasian Performing Right Association Limited v Jain (1990) 26 FCR 53 followed/distinguished
Australasian Performing Right Association Ltd v Metro on George Pty Ltd and Others (2004) 61 IPR 57 followed/distinguished
Australian Tape Manufacturers Association Ltd and Others v The Commonwealth of Australia (1993) 177 CLR 480 followed
Avel Proprietary Limited v Multicoin Amusements Proprietary Limited and Another (1990) 171 CLR 88 followed
C J Redman Constructions Pty Ltd v Tarnap Pty Ltd [2006] NSWSC 173 referred to
Canadian Pacific Tobacco Limited and Another v Stapleton (1952) 86 CLR 1 referred to
CBS Songs Ltd and Others v Amstrad Consumer Electronics PLC and Another [1988] AC 1013 referred to
Commercial Union Assurance Company of Australia Ltd v Ferrcom Pty Ltd and Another (1991) 22 NSWLR 389 distinguished
Computermate Products (Aust) Pty Ltd v Ozi-Soft Pty Ltd and Others (1988) 20 FCR 46 followed
Cooper v Universal Music Australia Pty Ltd and Others (2006) 156 FCR 380 followed/distinguished
Corbis Corporation v Amazon.com, Inc 351 FSupp2d 1090 (WD Wash 2004) considered
The Corporation of the City of Adelaide v The Australasian

Performing Right Association Limited (1928) 40 CLR 481 considered
CSR Limited v Eddy (2006) 226 CLR 1 referred to
E-Talk Communications Pty Ltd & Anor v Universal Music Pty Ltd & Ors [2007] HCATrans 313 considered
Falcon v Famous Players Film Company [1926] 2 KB 474 cited
Harlan Ellison v Stephen Robertson 189 FSupp2d 1051 (CD Cal 2002) considered
Harlan Ellison v Steven Robertson 357 F3d 1072 (9th Cir 2004) considered
In Re: Aimster Copyright Litigation 334 F3d 643 (7th Cir 2003) questioned
In Re: Aimster Copyright Litigation 252 FSupp2d 634 (ND Ill 2002) considered
Moorhouse & Angus and Robertson (Publishers) Pty Ltd v University of New South Wales (1974) 3 ALR 1 distinguished
Nationwide News Pty Ltd and Others v Copyright Agency Limited (1996) 65 FCR 399 followed
Nominet UK v Diverse Internet Pty Ltd and Others (2004) 63 IPR 543 cited
Perfect 10, Inc v *CCBill, LLC* 340 FSupp2d 1077 (CD Cal 2004) considered
Perfect 10, Inc v CCBill, LLC 481 F3d 751 (9th Cir 2007) considered
Perfect 10, Inc v Cybernet Ventures, Inc 213 FSupp2d 1146 (CD Cal 2002) considered
Performing Right Society, Limited v Ciryl Theatrical Syndicate, Limited [1924] 1 KB 1 cited
Recording Industry Association of America Inc v Verizon Internet Services Inc 351 F3d 1229 (DC Cir 2003) referred to
Roadshow Films Pty Ltd v iiNet Limited (No 2) [2009] FCA 1391 referred to
Roadshow Films Pty Ltd and Others (ACN 100 746 870) v iiNet Limited (ACN 068 628 937) (2009) 81 IPR 99 referred to
Sony Corporation of America v Universal City Studios Inc 464 US 417 (1984) cited
TCN Channel Nine Pty Ltd v Network Ten Pty Ltd (No 2) (2005) 145 FCR 35 cited
Telstra Corporation Limited v Australasian Performing Right Association Limited (1997) 191 CLR 140 discussed
Universal Music Australia Pty Ltd and Others v Cooper and Others (2005) 150 FCR 1 followed/distinguished
Universal Music Australia Pty Ltd and Others v Sharman License Holdings Ltd and Others (2005) 65 IPR 289 followed/distinguished
The University of New South Wales v Moorhouse and Another (1975) 133 CLR 1 followed

WEA International Inc and Another v Hanimex Corporation Ltd (1987) 17 FCR 274 followed

Date of hearing:	6 – 9, 12 – 15 October 2009, 2 – 6, 9 – 11, 13, 19, 24, 26 November 2009
Place:	SYDNEY
Division:	GENERAL DIVISION
Category:	Catchwords
Number of paragraphs:	636
Counsel for the Applicants:	Mr A. J. L. Bannon SC with Mr J. M. Hennessy and Mr C. Dimitriadis
Solicitor for the Applicants:	Gilbert + Tobin
Counsel for the Respondent:	Mr R. Cobden SC with Mr R. P. L. Lancaster SC and Mr N. R. Murray
Solicitor for the Respondent:	Herbert Geer

IN THE FEDERAL COURT OF AUSTRALIA
NEW SOUTH WALES DISTRICT REGISTRY
GENERAL DIVISION **NSD 1802 of 2008**

BETWEEN:	**ROADSHOW FILMS PTY LTD (ACN 100 746 870)** **First Applicant**
	THE PARTIES IN THE ATTACHED SCHEDULE I **Second Applicant to Thirty-Fourth Applicant**
AND:	**IINET LIMITED (ACN 068 628 937)** **Respondent**

JUDGE:	**COWDROY J**
DATE OF ORDER:	**4 FEBRUARY 2010**
WHERE MADE:	**SYDNEY**

THE COURT ORDERS THAT:

1. The Amended Application be dismissed.

2. Subject to Order 3 and 4, the Applicants pay the costs of the Respondent, including costs thrown away as a result of the Applicants' abandoning the primary infringement claim against the Respondent.

3. Any party or person applying for an order for costs different to that provided by Order 2 is to notify the Court within 14 days in which event Order 2 will be vacated and in lieu costs will be reserved.

4. If any application for costs is made as provided in Order 3 the parties and/or persons are to consult and prepare consent directions for the filing of submissions and, if required, for a hearing on costs.

Note: Settlement and entry of orders is dealt with in Order 36 of the Federal Court Rules. The text of entered orders can be located using eSearch on the Court's website.

IN THE FEDERAL COURT OF AUSTRALIA
NEW SOUTH WALES DISTRICT REGISTRY
GENERAL DIVISION **NSD 1802 of 2008**

BETWEEN:	**ROADSHOW FILMS PTY LTD (ACN 100 746 870)** **First Applicant**
	THE PARTIES IN THE ATTACHED SCHEDULE I **Second Applicant to Thirty-Fourth Applicant**
AND:	**IINET LIMITED (ACN 068 628 937)** **Respondent**

JUDGE:	**COWDROY J**
DATE:	**4 FEBRUARY 2010**
PLACE:	**SYDNEY**

REASONS FOR JUDGMENT

PART A: INTRODUCTION

1 These proceedings primarily concern the question whether an Internet Service Provider ('ISP') authorises the copyright infringing acts of its subscribers or users of its services if those subscribers or users, without licence, download films in respect of which copyright is claimed. The judgment is structured as follows,

PART A: INTRODUCTION ..... [1]
The parties ..... [2]
The proceedings ..... [5]
The Amended Application ..... [6]
The FASOC ..... [9]
The Amended Defence of the respondent ..... [17]
The applicants' Reply ..... [37]
Structure of judgment ..... [41]
PART B: TECHNICAL BACKGROUND ..... [43]
The internet ..... [44]
IP addresses and packets ..... [44]

NAT ..... [49]
Physical facilities ..... [52]
Dynamic IP addresses ..... [54]
The BitTorrent protocol ..... [56]
BitTorrent client ..... [58]
.torrent file ..... [61]
Hashes ..... [62]
Location of .torrent files ..... [68]
The tracker ..... [69]
Summary ..... [70]
How are pieces shared? ..... [74]
Conclusion ..... [78]
PART C: THE EVIDENCE ..... [79]
Role of AFACT ..... [80]
AFACT witness – Aaron Guy Herps ..... [83]
Downloading films and television programs ..... [85]
AFACT witness – Gregory Donald Fraser ..... [91]
AFACT witness – Neil Kevin Gane ..... [93]
Evidence of copyright infringement ..... [94]
Investigations of online piracy in Australia ..... [96]
Expert witness – Nigel John Carson ..... [105]
DtecNet witness – Thomas John Sehested ..... [109]
DtecNet witness – Kristian Lokkegaard ..... [110]
Collection of data using DtecNet Agent ..... [113]
Michael John Williams ..... [114]
'Repeat infringer bundles' ..... [115]
Bundles involving the RC-20 accounts ..... [116]
DNS Lookups ..... [118]
The iiNet subscriber accounts ..... [122]
Studio witnesses ..... [126]

Respondent's witness – Michael Martin Malone ..... [129]
Findings as to the credit of Mr Malone ..... [132]
WESTNET ISSUE ..... [137]
REPEAT INFRINGER POLICY ..... [155]
TELCO ACT DEFENCE ..... [159]
VARIOUS OTHER STATEMENTS OF MR MALONE ..... [163]
PROSECUTION OF MR HERPS ..... [167]
'Compelling evidence' ..... [172]
Freezone ..... [181]
'Robot' notices ..... [192]
Respondent's witness – Stephen Joseph Dalby ..... [193]
Credit of Mr Dalby ..... [195]
PREPARATION OF AFFIDAVIT ..... [197]
LACK OF UNDERSTANDING OF AFACT NOTICES ..... [203]
TELCO ACT ISSUE ..... [212]
Submissions regarding the respondent's failure to call more witnesses ..... [216]
Respondent's witness – David Buckingham ..... [221]
The respondent's financial interests – 'The iiNet business model' ..... [224]
Is 'bandwidth', 'downloading' or 'quota use' necessarily infringing? ..... [239]
Proof of infringement – catalogue vs identified films ..... [251]
PART D: PRIMARY INFRINGEMENT ..... [253]
The authorisation of acts, not of persons ..... [258]
Nature of the primary infringements ..... [264]
The dispute ..... [270]
'Make available online' a substantial part of the film to the public ..... [272]
Repeat infringers? ..... [276]
How DtecNet produces multiple allegations of infringement ..... [279]
Correct construction of 'make available online' ..... [285]
'Electronically transmit' a substantial part of the film to the public ..... [301]
'Substantial part' ..... [302]

'To the public' ..... [307]
The solution ..... [310]
Who makes the communication? ..... [319]
Were the applicants' investigators licensed? ..... [326]
STUDIO WITNESSES' EVIDENCE ..... [330]
MR GANE'S EVIDENCE ..... [334]
MOORHOUSE ..... [338]
Did s 104 of the Copyright Act apply? ..... [345]
Make a copy of a substantial part of a film ..... [346]
Copies from BitTorrent ..... [347]
Further copies made on physical media ..... [349]
Conclusion ..... [356]
PART E1: AUTHORISATION ..... [357]
Judicial consideration of authorisation ..... [359]
Kazaa ..... [360]
Cooper ..... [363]
The 'means' of infringement ..... [367]
Moorhouse ..... [367]
GIBBS J ..... [369]
JACOBS J (MCTIERNAN ACJ AGREEING) ..... [376]
CONCLUSION ..... [381]
Importance of factual context in decisions following Moorhouse ..... [383]
APRA CASES ..... [385]
TECHNOLOGY CASES ..... [389]
Did the respondent provide the 'means' of infringement? ..... [400]
Section 101(1A) considerations ..... [415]
Section 101(1A)(a) Power to prevent ..... [417]
AUTHORITY ..... [418]
DID THE RESPONDENT HAVE THE POWER TO PREVENT THE INFRINGEMENTS? .. [424]
APPLICANTS' SUBMISSIONS THAT THE RESPONDENT DID HAVE THE POWER [425]

TO PREVENT INFRINGEMENTS .....

THE COURT'S CONSIDERATION ..... [436]

TELCO ACT ..... [443]

CONCLUSION ..... [444]

Section 101(1A)(b) Relationship ..... [446]

Section 101(1A)(c) Reasonable steps ..... [454]

WHAT IS THE ROLE OF REASONABLE STEPS? ..... [455]

WERE THERE REASONABLE STEPS THE RESPONDENT COULD HAVE TAKEN? ..... [458]

Other considerations – Knowledge of infringements ..... [461]

Other considerations – Encouragement of infringement ..... [473]

Failure to act ..... [475]

20 November 2008 press release ..... [476]

'Golden Girls *advertisement*' ..... [480]

Encouragement to upgrade ..... [485]

Other considerations – Inactivity or indifference ..... [487]

Did the respondent sanction, approve, countenance the infringements of the iiNet users? ..... [493]

Approve ..... [495]

Sanction ..... [496]

Countenance ..... [497]

Findings ..... [500]

Conclusion on authorisation ..... [505]

PART E2: THE TELCO ACT DEFENCE ..... [508]

The Telco Act ..... [511]

Operation of s 276 ..... [513]

Does the information required to be used satisfy s 276(1)(a)? ..... [517]

Does the information required to be used satisfy s 276(1)(b)? ..... [518]

Exceptions ..... [527]

Operation of s 279 ..... [528]

Operation of s 280 ..... [533]

Operation of s 290 ..... [540]
Operation of s 289 ..... [543]
Conclusion ..... [555]
PART E3: SECTION 112E OF THE COPYRIGHT ACT ..... [556]
Section 112E ..... [557]
Judicial Authority ..... [560]
Kazaa ..... [560]
Cooper 150 FCR 1 ..... [563]
Cooper 156 FCR 380 ..... [565]
The Court's interpretation of s 112E ..... [568]
Can the respondent take advantage of s 112E? ..... [576]
Conclusion ..... [579]
PART F: SAFE HARBOUR PROVISIONS ..... [580]
Interaction between the safe harbour provisions and copyright authorisation ..... [585]
What is a repeat infringer policy? ..... [590]
US precedent on safe harbor provisions ..... [595]
REQUIREMENTS OF THE POLICY ..... [597]
IMPLEMENTATION OF THE POLICY ..... [602]
CONCLUSIONS ..... [607]
Did the respondent have a repeat infringer policy? ..... [611]
Has the respondent reasonably implemented such a policy? ..... [620]
Other issues ..... [633]
Conclusion ..... [634]
PART G: CONCLUSION ..... [635]
SCHEDULE I – THE APPLICANTS
SCHEDULE II – THE IDENTIFIED FILMS

The parties

2 In these proceedings there are 34 applicants which comprise most of the major film studios and their exclusive licensees in Australia. In these proceedings the applicants acted together as effectively one party.

3 Attached to this judgment as Schedule I is a list of the applicants. Each of the applicants are the owners and exclusive licensees of copyright in a large number of cinematograph films in the form of films and television programs (the Court will refer to both these television programs and films as 'films'). A sample of 86 such films for which copyright ownership and subsistence has been proved and upon which the Court has heard evidence are identified in Schedule II of this judgment and these 86 films will be referred to as the 'identified films'. When referring to the broader catalogue of films of the applicants, the term 'catalogue films' will be used. For further discussion of this issue, see [252] below.

4 The respondent, iiNet, is an ISP. Mr Malone, the CEO of the respondent and a witness in these proceedings, commenced the respondent's business operations in his parent's garage in Perth in October 1993. The business was incorporated in March 1995. In September 1999 the respondent became a public company and listed on the Australian Stock Exchange. At the time of its public listing, the respondent had approximately 19,000 subscribers. This has now risen to approximately 490,000 subscribers. Following Telstra and Optus, the respondent is the third largest ISP in Australia.

The proceedings

5 The proceedings commenced on 20 November 2008 by way of Application and Statement of Claim. Subsequently, following amendments to both documents, the litigation was conducted upon the basis of an Amended Application and a Further Amended Statement of Claim ('FASOC') filed in the Federal Court Registry on 11 May 2009 pursuant to leave granted by the Court. The Court will now turn to these pleadings.

The Amended Application

6 The Amended Application seeks declarations that the respondent has infringed the copyright of films contained in each of the applicants' respective film catalogues by authorising the making in Australia of copies of, and by authorising the communication in Australia to the public of, the whole or a substantial part of those films without the licence of the applicants. Further, a declaration is sought that the respondent carried out such infringing acts flagrantly and that such infringements, together with other likely infringements, were conducted on a commercial scale for the purpose of s 115(5)(d) of the *Copyright Act 1968* ('the Copyright Act').

7 By way of further relief, the applicants seek injunctions permanently restraining the respondent from infringing the copyright in any of the films contained in the catalogue of the applicants, and an order requiring the respondent to take all reasonable steps to disable access to any online location outside Australia that has been used to infringe the applicants' copyright. An order is also sought requiring the respondent to terminate specified accounts of the respondent's subscribers who have engaged in or who have continued to engage in acts of copyright infringement involving the applicants' films.

8 Lastly, an order is sought for damages or, alternatively (at the election of the applicants), an account of profits pursuant to s 115(2) of the Copyright Act; additional damages pursuant to s 115(4) of the Copyright Act (applicable to conduct which is found to be flagrant); relief under s 115(6) of the Copyright Act which entitles the Court to have regard to the likelihood of other infringements (as well as the proven infringement) in determining what relief should be granted; and costs and interest.

The FASOC

9 The Court will now summarise the FASOC and, for convenience, the paragraphs referred to hereunder are those set out in such pleading.

10 Paragraphs 1-13 recite the relevant details of incorporation of each of the applicants and paragraph 14 refers to the incorporation of the respondent. Paragraphs 15-56 inclusive refer to the applicants' claim that they are the owners or exclusive licensees of the films contained in their respective catalogues, that such films are cinematograph films and that copyright subsists in such films. Paragraphs 57 and 58 refer to the provision of internet services by the respondent to its subscribers.

11 The acts of 'primary' infringement (see [256] below) of copyright are alleged in paragraphs 59-62. In such paragraphs the applicants claim that from a date unknown to them, but at least since July 2008, the respondent's subscribers and other persons accessing the internet by means of the respondent's internet service (henceforth referred to together as the 'iiNet users') have, in Australia, whilst accessing the internet by means of the respondent's internet services, 'made available online' to other persons; 'electronically transmitted' to other persons; and made copies of, the whole or a substantial part of the identified films and

the catalogue films without their licence. Further, or alternatively, it is alleged that such iiNet users have copied such films and thereafter made further copies without licence on DVD or other physical storage media for the purpose of watching, storing or distributing those films.

12 Paragraphs 63-67 allege that the respondent authorised the infringement of the iiNet users. It is alleged that the respondent knew or had reason to suspect that the iiNet users were engaged in, and were likely to continue to engage in, such conduct; took no action in response to notifications sent on behalf of the applicants which claimed that iiNet users were engaging in the conduct referred to above; offered encouragement to iiNet users to engage in or to continue to engage in the conduct; failed to enforce the terms and conditions of its Customer Relationship Agreement ('CRA') by which its internet services were provided; continued to provide services to those subscribers who were engaging in the conduct complained of; and through the respondent's inactivity and indifference, permitted a situation to develop and continue whereby iiNet users engaged in such conduct.

13 Paragraph 64 pleads in the alternative that the respondent had the power to prevent the infringements and continuing infringements from occurring; had a direct and commercial relationship with its subscribers which enabled it to take action against those subscribers who engaged in the infringing conduct; and yet took no steps or adequate steps to prevent or avoid infringement.

14 Paragraph 67A alleges that the respondent further, or in the alternative, has, in the course of providing its internet services, provided facilities for the intermediate and transient storage or, alternatively, caching of copyright material, namely the applicants' films. Paragraph 67B claims that by reason thereof the respondent has made copies of the whole or a substantial part of the identified films and the catalogue films. Paragraph 67D alleges that the copies were made without the licence of the applicants and therefore the respondent has infringed the copyright in the identified films and the catalogue films. Such claim, being one of primary copyright infringement against the respondent, was abandoned by the applicants shortly before the hearing commenced on 6 October 2009. The applicants informed the Court of this fact in an email exchange on 30 September 2009.

15 Loss, damage and profits are claimed in paragraphs 68-74. The applicants claim that they have suffered or are likely to suffer loss and damage on a commercial scale and that by

reason of the infringements the respondent has accrued or is likely to accrue profits to itself and its business.

16 Injunctive relief is sought in paragraphs 76-77 to restrain the respondent from engaging in the infringing activities.

The Amended Defence of the respondent

17 Similarly to the applicants, the respondent was granted leave to file an Amended Defence on 8 May 2009. Such document was filed in the Federal Court Registry on 15 May 2009.

18 The respondent largely admits all matters regarding copyright subsisting in, and the applicants owning the copyright in, the identified films.

19 The respondent acknowledges that it provided at all relevant times, and continues to provide, telecommunications services to persons in Australia which are listed carriage services within the meaning of ss 7 and 16 of *Telecommunications Act 1997* (Cth) (the 'Telco Act'); says that such services were provided under terms and conditions of supply published by the respondent from time to time in its CRA; and that the provision of those services is subject to the statutory requirements of the Telco Act, the *Telecommunications (Interception and Access) Act 1979* (Cth) (the 'TIA Act'), the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth) and the *Broadcasting Services Act 1992* (Cth).

20 The respondent pleads that at all material times the services used by its subscribers and other persons in obtaining access to, and exchanging of data on, the internet were facilities for making or facilitating the making of communications within the meaning of s 112E of the Copyright Act. Further, the respondent pleads that at all material times such facilities or services were provided for transmitting, routing or providing connections for copyright material or for the intermediate and transient storage of copyright material in the course of transmission, routing or provision of connections within the meaning of s 116AC of the Copyright Act.

21 The respondent states that it provided its subscribers with access to the internet and that to enable access to the internet the respondent allocated IP addresses for use by those subscribers; that as part of such services it charged its subscribers fees applicable to the relevant plan to which the subscriber subscribed; and that it derived no commercial advantage from its subscribers over and above the payment for such services.

22 The respondent initially did not admit the allegations made in paragraphs 59 and 60 of the FASOC regarding the infringing conduct of the iiNet users. However, by the '*Respondent's Statement of Nature of Case*' filed by the respondent on 9 April 2009, the respondent made clear that it conceded that, for the purposes of this hearing, the evidence filed by the applicants by that date showed that iiNet users infringed copyright by 'making the identified films available online' and making copies of those films. The respondent maintained its non-admission in regards to further copying described in paragraph 60 of the FASOC and denied that the evidence proved that the iiNet users 'electronically transmitted' the identified films.

23 The respondent's defence also alleges that if the infringing acts were committed, to the extent that those acts involved the activities of employees, agents, or other representatives of AFACT and/or of any of the applicants, such acts were done with the licence of the relevant applicants or alternatively were done in circumstances which, by virtue of the application of s 104 of the Copyright Act, did not constitute infringement of copyright.

24 As to the alleged authorisation by the respondent of the acts of the iiNet users referred to in paragraphs 63 and 64 of the FASOC, if such alleged infringing acts occurred, the respondent replies:

> In answer to paragraphs 63 and 64 of the Further Amended Statement of Claim, iiNet:
>
> (a) …
>
> (b) says that it knew at all material times that a proportion of the internet traffic exchanged via its facilities comprised data exchanged via the BitTorrent protocol;
>
> (c) says that is knew at all material times that copyright owners have alleged that a proportion of BitTorrent internet traffic exchanged over the internet generally included content which was likely to infringe copyright;
>
> (d) says that the BitTorrent protocol has, and is known by the applicants to have,

many non-infringing uses and facilities;

25 The respondent pleads the following in further answer to paragraphs 63 and 64:

(i) It [the respondent] did not create the BitTorrent protocol or any BitTorrent software;

(ii) was, and is, not the operator of the BitTorrent protocol or any BitTorrent software;

(iii) has not, and does not, promote the BitTorrent protocol or any BitTorrent software other than for purposes that do not involve the infringement of the applicants' or any other party's copyright;

(iv) has not entered into any agreements with BitTorrent Inc. or any other BitTorrent related company;

(v) does not have a direct or commercial relationship with BitTorrent Inc. or any other BitTorrent related companies;

(vi) has not, and does not, encourage users to share files which infringe the applicants' or any other party's copyright;

(vii) did not, and does not, support the BitTorrent protocol or any BitTorrent software except for use in a non-infringing manner;

26 The respondent says it knew from 2 July 2008 of the allegations of copyright infringement being made on behalf of the applicants and that it took action in relation to the allegations.

27 However, the respondent pleads that the allegations were '*mere allegations of copyright infringement*' and that such allegations provided insufficient information to demonstrate the veracity of the allegations made and to allow the respondent to verify the allegations.

28 The respondent further pleads that it is a general purpose ISP and not a facility for 'making available', 'electronically transmitting' or copying cinematograph films. Further, the respondent pleads that it is required to comply with the legislation regulating communications passing over telecommunications networks and use of information relating to such communications as stipulated in Part 13 of the Telco Act and Chapter 2 of the TIA Act.

29 The respondent says it continued to provide its services to its subscribers subsequent to the allegations of copyright infringement being made against it and relies upon its contractual obligations with its subscribers. The respondent pleads that it did not sanction,

approve or countenance the conduct of any iiNet user which would result in the infringement of copyright as alleged.

30 Further, the respondent pleads that it did not have any relevant power within the meaning of s 101(1A)(a) of the Copyright Act or otherwise to prevent alleged infringing acts by iiNet users. It states that it had no 'relationship' within the meaning of s 101(1A)(b) of the Copyright Act with the users of its services who are not subscribers; pleads if it did have a relationship, such relationship was neither direct nor commercial; and pleads it does not know the identity of those users.

31 Further, the respondent pleads that it took reasonable steps to prevent or avoid the alleged infringing acts. Otherwise, the allegations against the respondent are denied.

32 The respondent also raises specific defences under the Copyright Act. The respondent relies upon s 112E of the Copyright Act which provides:

> **Communication by use of certain facilities**
>
> 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 an audio-visual item merely because another person uses the facilities so provided to do something the right to do which is included in the copyright.

33 Further, or in the alternative, the respondent pleads that if copyright infringement against it is proved, the conduct relied upon by the applicants was category A activity within the meaning of s 116AC of the Copyright Act. Section 116AC is contained in Division 2AA of Part V of the Copyright Act ('safe harbour provisions') which limits the remedies available against carriage service providers for infringement of copyright if certain conditions are fulfilled by the carriage service provider.

34 The respondent pleads that it has complied with those conditions in that it has not initiated any transmission of the films nor made any substantive modifications to any films other than as part of a technical process.

35 Further, the respondent submits that it has adopted and reasonably implemented a policy that provides for termination in appropriate circumstances of repeat infringers (as

required by condition 1 of item 1 of s 116AH(1) of the Copyright Act) and states that no relevant industry code exists (as referred to in condition 2 of item 1 of s 116AH(1) of the Copyright Act) to which the respondent can adhere.

36 In these circumstances, the respondent submits that even if the applicants were entitled to any relief (which is denied), such relief is limited to an order requiring the respondent to take reasonable steps to disable access to an online location outside Australia or requiring the respondent to terminate specified subscribers' accounts.

The applicants' Reply

37 The Reply filed in answer to the respondent's Defence (not the Amended Defence) acknowledges the respondent's pleading which alleges that the respondent is a carriage service provider within the definition of that word in the Telco Act and that the respondent is engaged in the provision of telecommunications services, including internet services, to members of the public in Australia.

38 The applicants admit that the BitTorrent protocol exists and is capable of use in the manner described in the applicants' particulars. The applicants also admit that there is no relevant industry code in force for the purpose of condition 2 of item 1 in the table in s 116AH(1) of the Copyright Act.

39 The applicants claim that if (which is denied) s 116AH(1) of the Copyright Act applies, the Court should make orders requiring the respondent to take all reasonable steps to disable access by iiNet users to online locations used to infringe copyright, and to require the respondent to terminate accounts of subscribers who have engaged in infringement or whose accounts have been used for infringement.

40 Otherwise the applicants join issue with the Defence. It should be noted that the filing of the Amended Defence did not require the filing of an Amended Reply.

Structure of judgment

41 The Court is mindful of the substantial length of this judgment. However, given the length of the trial (some 20 days), the length and detail of the closing submissions (over 800

pages, excluding hundreds of pages of tables, graphs and spreadsheets), and the obvious importance of these proceedings to the law of copyright both in this country and possibly overseas, the Court believes that all submissions made and arguments raised ought to be decided to give certainty and finality to the litigation (pending any appeal).

42 To assist the consumption and comprehension of this lengthy judgment, it has been divided into a number of parts, each addressing specific issues. To some extent there may be repetition, but this is unavoidable if the various parts of the judgment are to be readily comprehended. Part A [1]-[42] is the current part, the introduction. Part B [43]-[78] provides a succinct explanation of the operation of the internet and of the BitTorrent protocol. A comprehension of both is necessary to understand the subsequent findings. Part C [79]-[252] discusses important evidentiary issues in the proceedings. In Part D [253]-[356] the Court discusses and makes findings on the issue of whether the applicants have been successful in proving that iiNet users infringed their copyright. Part E1 [357]-[507] concerns the pivotal issue of these proceedings, namely whether the respondent can be said to have authorised any infringement by the iiNet users. Part E2 [508]-[555] concerns the specific issue of whether the Telco Act prohibited the respondent from acting on the AFACT Notices. Part E3 [556]-[579] concerns the issue of whether s 112E of the Copyright Act assists the respondent in these proceedings. Part F [580]-[634] concerns the issue whether the respondent can take advantage of the safe harbour provisions in Division 2AA of Part V of the Copyright Act. Finally, in Part G [635]-[636], the Court makes its conclusions. Following the conclusion, there are two schedules attached to the judgment. The first ('I') lists the second to thirty-fourth applicants in these proceedings and the second ('II') lists the identified films and their owners and/or exclusive licensees.

PART B: TECHNICAL BACKGROUND

43 This judgment proceeds into a significant amount of technical detail. In order to better understand the reasons given, a brief technical interlude into the operation of both the internet and the BitTorrent protocol is necessary. The Court will turn first to the internet and then to the BitTorrent protocol. The information in this technical interlude is derived from both the evidence given at trial and certain notorious facts of which the Court takes judicial notice.

The internet

IP addresses and packets

44 The internet is, in summary, a network of networks of computers. In order for those computers to be able to communicate with each other, they have to be speaking the same language. Protocols facilitate this process. Protocols could be described as languages or, alternatively, sets of rules for computers. If two computers obey these rules, they will be able to understand each other and communicate. The two primary protocols by which communication is effected between computers on the internet are the Internet Protocol ('IP'), and the Transmission Control Protocol ('TCP'). TCP is not relevant for these proceedings and will not be discussed further.

45 Data that is sent by means of the IP is 'packetised', that is, the data to be communicated is broken up into small packets and then sent by means of the IP. Each packet contains a header (akin to an envelope) containing information identifying the address or location from which the packet is sent and to which the packet is to be sent and other information not presently relevant. The packet itself contains the data which is akin to the letter within an envelope. The IP protocol effects communication between computers by means allocating addresses to the sending and receiving computers and then sending the packets of data from one address to another, in many ways analogous to the mail.

46 Such IP addresses are sold in blocks to ISPs, who then individually allocate them to their subscribers to enable the subscribers to connect to the internet. The body which allocates IP addresses to Australian ISPs is the Asia-Pacific Network Information Centre or APNIC. The identity of the ISP to which certain IP addresses have been allocated is public information.

47 The addresses used by the IP are known as IP addresses. They are a number rendered in binary code but, for the benefit of readability by persons, they are converted into a number of 4 groups of 3 digits separated by a full stop, for example, 192.168.111.123. The IP addresses in evidence in these proceedings are in this form.

48 In most situations, packets of data are not sent directly from one location to another, largely because each computer on the internet is not connected directly to every other

computer on the internet. Rather, each computer is linked to other computers which are then in turn connected to other computers and so on. That is why the internet is not a network of computers; it is a network of networks of computers. Further, not all packets dispatched from one computer travel to the same destination by means of the same path.

NAT

49 A further important concept is Network Address Translation ('NAT'). This allows a router (which is essentially a device which can 'route' data between a network of computers) to take one internet connection and split it between a number of computers. Such routers also allow a number of computers to communicate with each other, creating a network. In this scenario, one internet connection comes through a modem into a router. That router then distributes the data to the computers which are connected to it via ethernet (network) cables, or, alternatively, wirelessly by means of Wi-Fi. This internal network prevails in many households and most businesses.

50 Each computer connected to the router is assigned an IP address by the router in the same format as that used in the internet. However such IP addresses are private, that is, they are known only to the computers on that network. The IP address of a particular computer is not broadcast to the internet. This allows the number of computers connected to the internet to be dramatically increased, because each computer does not need its own public IP address allocated by an ISP. Rather, the computer is connected to the internet through a router, with the router being assigned the public IP address by the ISP. This public IP address is the only address that is seen by other computers on the internet.

51 Therefore, one can know the location of a connection to the internet by means of a public IP address, but a public IP address does not necessarily relate to a specific person or specific computer. There may only be one computer connected to the internet through a public IP address. Equally, there may be hundreds. One cannot know which is the case from outside that particular network. For the balance of this judgment, unless otherwise indicated, the term IP address will refer to a public IP address.

Physical facilities

52 As mentioned, IP addresses are allocated to subscribers by ISPs. ISPs also connect subscribers to the internet by means of physical infrastructure. Such infrastructure may be owned by multiple ISPs. For a subscriber of the respondent with an ADSL2+ (a type of internet connection) plan, that subscriber's connection to the internet outside Australia, generally speaking, occurs by the means discussed below.

53 The household computer sends data to the router, which then forwards the data to the ADSL2+ modem. This ADSL2+ modem then transmits data down the copper phone lines to an exchange. The copper phone lines and exchange are owned by Telstra. Exchanges are local hubs of copper telephone wire connections. At the exchange, the copper wire terminates into a Digital Subscriber Line Access Multiplexer ('DSLAM'), which is owned and provided by the respondent. The DSLAMs allow many copper connections to be aggregated together. The data is then sent from this exchange via the DSLAM to an iiNet data centre, which is a larger facility where connections from multiple exchanges are aggregated. Where the sending computer is based outside Sydney, for example, in Western Australia, the data would need another leap from the city data centre in question (for example, Perth) to Sydney, Sydney being the location of the connection to the rest of the world. This connection occurs from the Sydney data centre to the rest of the world by means of undersea optical fibre cables.

Dynamic IP addresses

54 For most of the respondent's subscribers, the IP address provided to them to access the internet is not fixed; rather, it is dynamically assigned. This means the IP address by which a computer is connected to the internet changes over time. The respondent provides a fixed ('static') IP address for all subscribers on business plans.

55 As already discussed, protocols are the means by which computers communicate. While TCP and IP have been mentioned, there are many others, for example, smtp (email), ftp (file transfer), http (world wide web), VOIP (voice) and BitTorrent. As already mentioned, the latter protocol is central to the current proceedings.

The BitTorrent protocol

56 The BitTorrent protocol is essentially a scheme for a highly efficient and decentralised means of distributing data across the internet. The term ‘decentralised’ is used in this context in contradistinction to the traditional model of data distribution which is the client/server model. In that model one computer which has the data (the ‘server’) sends that data to another computer which requests it (the ‘client’), often by means of the http or ftp mentioned above. The BitTorrent protocol operates on a different basis. It operates on a ‘peer to peer’ (‘p2p’) basis whereby all the computers seeking data participate in the distribution of it.

57 The BitTorrent protocol is a set of rules, or, in layman’s terms, a blueprint. It specifies what needs to be done to implement a system of data distribution. It has a number of constituent parts which will be explained in more detail below.

BitTorrent client

58 The first part of the BitTorrent protocol is the BitTorrent client. The BitTorrent client is a computer program or software which allows a person to access groups of computers sharing a particular .torrent (explained below) file. These groups of computers are known as ‘swarms’. Each computer in a swarm is known as a ‘peer’.

59 The BitTorrent client can have no operation by itself, as it needs to be provided with information in order to fulfil its role. This information comes from a .torrent file.

60 There are a number of BitTorrent clients provided free of charge from a variety of different organisations. The client referred to primarily in these proceedings was uTorrent (pronounced ‘you-torrent’) which is the most popular BitTorrent client. Other BitTorrent clients include Vuze, and, rather confusingly, the BitTorrent Client, which is the BitTorrent client of BitTorrent Inc, such company being founded by Bram Cohen who created the BitTorrent protocol in 2001. Each BitTorrent client operates in the same basic way, as it must comply with the requirements of the BitTorrent protocol in order to be able to function as a part of it. However, as well as these basic functions, different clients may have different graphical user interfaces, a search function for .torrent files, more advanced features and so on.

.torrent file

61 The second part of the BitTorrent protocol is the .torrent file. The term '.torrent' refers to a file extension. File extensions, such as .doc, .avi, .mp3, .pdf, .exe and so on do nothing more than associate a particular file with a particular purpose. For example, a .doc file is a document, .avi is a film file (the files in question in these proceedings were frequently .avi files), and .mp3 is a music file (the subject of the proceedings in *Universal Music Australia Pty Ltd and Others v Cooper and Others* (2005) 150 FCR 1 ('*Cooper* 150 FCR 1') and *Universal Music Australia Pty Ltd and Others v Sharman License Holdings Ltd and Others* (2005) 65 IPR 289 ('*Kazaa*')). This .torrent file contains the information necessary for the BitTorrent client to contact and participate in a swarm. It is important to emphasise that the .torrent file does not contain the underlying data of a film or television program. Rather, the .torrent file contains the name of the file sought, the size of the file, the hash value of the file, the hash value of the pieces of the file, and the location of the tracker. Before moving on to explain the tracker, the third part of the BitTorrent protocol, an aside into hashes is necessary.

Hashes

62 The BitTorrent protocol operates by breaking up large files, such as film files (which are usually many hundreds of megabytes or a few gigabytes) into smaller parts ('pieces'). This is similar in principle to the means by which data is transferred across the internet, as discussed at [45] above.

63 As an aside, a 'byte' is a term that refers to a certain amount of data, namely 8 'bits'. A bit is either a zero or a one, given that computers compute by means of binary code. A 'kilobyte' is 1024 bytes, a 'megabyte' is 1024 kilobytes and a 'gigabyte' is 1024 megabytes.

64 The size of the pieces to which BitTorrent breaks a file into varies, but the evidence suggests that film files are often divided into pieces which are 512 kilobytes. These pieces will usually be larger than packets, which, as mentioned, are the mechanism by which data is transferred across the internet.

65 Such pieces are shared between the individual peers in a swarm. Over time, pieces are requested and received by the BitTorrent client from various other peers and are ultimately assembled together like a large jigsaw into the film file. In order to ensure that

each piece is received correctly, and that the data is not corrupted, the BitTorrent client consults hash values for each piece ('piece hashes'). A hash value is a means of converting a large amount of data into a smaller value and it is a mathematical function of its input, that is, an identical input equals an identical hash. This means a hash can fulfil the function of an identifier of data. The input in this circumstance comes from the data of the file being shared as a whole or a piece of that file. As mentioned, the .torrent file contains the details of the piece hashes of all the individual pieces of the file in question. When the BitTorrent client receives a piece of the file from another peer in the swarm, it checks that the piece hash of the piece is identical to the piece hash for that piece in the .torrent file. If it is, the BitTorrent client knows that the piece is the correct piece and was correctly received. If it is not, it is discarded and the requested piece is sought again.

66 The 'file hash' is different from the piece hash. While the piece hash is a mathematical function of the data of a particular piece, the file hash is the mathematical function of the data of the underlying file as a whole being shared in a swarm. The term 'file' is being used in a general sense in this context. A particular swarm may be sharing one file (in the case of an .avi film) or a number of files (for example, the individual songs on a CD in .mp3 format). The file hash applies to what is being shared as a whole, and serves as a mechanism of identifying what file is in each swarm. For example, the film *The Dark Knight* might be available in many different digital versions (and therefore in many different swarms). One version may be high quality (for example Blu-Ray quality), one lower quality (for example, DVD quality). Each version, and therefore each swarm, will have its own file hash, even though the underlying content, for example, *The Dark Knight*, is the same. This results from the fact that while the film is the same in each example, the underlying data is different, and therefore the file hash (which is a function of the data) is different.

67 The file hash is used by the applicants to show that a particular swarm is sharing one of their films, because they can watch a copy of the film with that file hash, identify it as their own, and then know that any copy with that file hash would be the same, because if the underlying file were different it would have a different file hash.

Location of .torrent files

68 The .torrent files are made available for download from a litany of sources. Some examples discussed in these proceedings include The Pirate Bay (http://thepiratebay.org) and MiniNova (http://www.mininova.org). Such sites have a search function which enables a person to search for the file that they want, whether it be a film such as *The Dark Knight*, or a television program such as *Lost*. There are also private sites like Demonoid (http://www.demonoid.com) which provide a similar service, but only do so for registered members. There are also a number of specialist sites that provide .torrent files for specific interests. Not all .torrent files relate to copyright infringing material.

The tracker

69 The third part of the BitTorrent protocol is the tracker. The tracker is a computer program on a server made available for contact by BitTorrent clients by means of a Universal Resource Locator ('URL') (in layman's terms, a web address). As mentioned, such URL is found in the .torrent file. This tracker monitors the particular swarm to which it is attached and monitors the IP addresses of peers in the swarm. The BitTorrent client, when provided with the location of the tracker by the .torrent file, contacts the tracker to request the IP addresses of peers in the swarm. The tracker then provides that information to the BitTorrent client. This allows the BitTorrent client to contact those peers directly (by their IP address) and request pieces of the file from them, and share pieces of the file with them.

Summary

70 To use the rather colourful imagery that internet piracy conjures up in a highly imperfect analogy, the file being shared in the swarm is the treasure, the BitTorrent client is the ship, the .torrent file is the treasure map, The Pirate Bay provides treasure maps free of charge and the tracker is the wise old man that needs to be consulted to understand the treasure map.

71 Whilst such an analogy grossly oversimplifies the situation it will suffice for present purposes. It demonstrates that all of the constituent parts of the BitTorrent protocol must work together before a person can access the file sought. In this judgment the Court will refer to all the constituent parts together as the 'BitTorrent system'.

72 Such analogy also demonstrates that a number of deliberate steps are required to be taken by a person to bring about the means to infringe the applicants' copyright. The person must download a BitTorrent client like Vuze, seek out .torrent files related to copyright material from websites, and download those .torrent files and open them in their BitTorrent client. Thereafter, the person must maintain connection to the internet for as long as is necessary to download all the pieces. The length of this downloading process will depend on the size of the file, the number of peers in the swarm and the speed of those peers' internet connections.

73 The BitTorrent protocol is able to efficiently distribute data because each peer is connected to many other peers, the file is split into many small pieces, and peers download pieces from other peers as well as uploading pieces. The BitTorrent logic operates so as to ensure that the rarest piece in a swarm is the first to be sought after, to average out the availability of pieces and minimise blockage or bottleneck which would occur if there were certain pieces of the file that many peers requested. By this mechanism the traditional problem with the client/server model is obviated. Under the client/server model, if there are many clients, the server has to provide the data to all of them which means that, given a fixed amount of capacity to provide data, that capacity has be shared amongst all the clients seeking that file. In layman's terms, this means the more persons that seek a file, the slower each person receives it. However, in the BitTorrent model, generally speaking, the more people wanting a file and therefore the bigger the swarm, the faster each individual peer receives the file. It is a highly sophisticated and efficient means of distributing data.

How are pieces shared?

74 For the purposes of these proceedings, a deeper understanding of the communication between the peers is required and such understanding will proceed by means of example.

75 In this example, the person has sought a .torrent file related to the film *The Dark Knight*: TheDarkKnight.avi. Such .torrent file was found on The Pirate Bay, and has been downloaded. The .torrent file has been opened in the BitTorrent client uTorrent. Upon opening the file, uTorrent will contact the tracker, seeking details about the swarm sharing that file, particularly the IP addresses of peers in that swarm. This initial contact is called 'scraping'. Once uTorrent has the IP addresses it can contact those peers directly. It does so

in a process called handshaking. Once this process is completed the peers can communicate directly.

76 The person in this scenario will not, initially, have any pieces of the TheDarkKnight.avi, but uTorrent will know because of the .torrent file all of the pieces it needs to obtain, and the piece hashes of those pieces. uTorrent will query the peers to which it is connected, in order to ascertain which pieces of the TheDarkKnight.avi those peers have. Some peers will have the whole of the TheDarkKnight.avi, and therefore all pieces will be available. These peers are known as ‘seeders’. Other peers may have less than the whole file because they are still in the process of downloading it, but they will still be able to share the pieces that they have.

77 Once the tracker is interrogated, uTorrent can determine which pieces are the rarest, and will therefore request those. As stated above, pieces are not downloaded in sequence; they are downloaded out of sequence, rarest first, and assembled together later. uTorrent will request a particular piece from another peer who is known to have it. This peer then decides whether or not to share it. Generally speaking, the only reason why a peer would refuse to share a piece would be that it had too many other peers connected to it. The assumption is in favour of sharing. If the peer decides to share the piece it will transmit the piece to the requesting peer’s computer. uTorrent will check the piece by means of the piece hash and, if such check is positive, accept the piece. Once this piece is received, uTorrent can then transmit that piece to other peers that request it. This process obviously occurs rapidly, with multiple peers and multiple pieces, and it is entirely automatic. From the point of view of the person, they simply see the file downloading, though they can, if desired, investigate in uTorrent the detail of the transmissions that are occurring. Over time uTorrent will receive all the pieces and the TheDarkKnight.avi will be assembled together. At this point in time the person will become a seeder, because they are sharing the whole file with the swarm. The default, that is, standard setting of uTorrent will result in the person sharing the file with the swarm until uTorrent is closed, or the .torrent file is removed from uTorrent. If the .torrent file is not removed and uTorrent is reopened, uTorrent will continue to share the file with the swarm.

Conclusion

78 The above explanation and examples are sufficient to enable an understanding of the internet and the BitTorrent protocol for the purpose of these proceedings. With that understanding, the Court will now address the evidence.

PART C: THE EVIDENCE

79 There has been an extensive amount of evidence placed before the Court in these proceedings. Evidence was given over ten days of the hearing. There were 30 affidavits read during the proceedings and 151 exhibits were tendered. It is impossible and unnecessary to refer to all the evidence that was placed before the Court. Suffice to say the Court has read and considered all the evidence. Each of the witnesses who have provided evidence will be discussed in the following part of the judgment, as well as the key evidentiary issues arising.

Role of AFACT

80 The Australian Federation Against Copyright Theft ('AFACT'), though not actually an applicant in these proceedings, has nonetheless played a central role in the collection of evidence on behalf of the applicants for this trial. AFACT is an organisation set up for the purposes of benefiting its members. Those members apparently include all of the applicants (or at least certain affiliate companies of each of the applicants) and other companies engaged in the film production industry.

81 The exact nature of the relationship between the applicants and AFACT is not clear. Mr Gane, the Executive Director of AFACT, suggested that there was no formal membership process by which one can become a member of AFACT, whether by application or agreement. Village Roadshow was an exception. What is clear is that the members of AFACT provide its budget and decide on its business plan, that is, what investigations and activities it will undertake.

82 The Motion Picture Association ('MPA') and the Motion Picture Association of America ('MPAA') have a membership of the major American film studios. They are not associated with AFACT by any formal written agreement. However, AFACT does report to the regional branch office of the MPA which is based in Singapore. In respect of operations

in the Asian region, the Singapore office of the MPA prepares a business plan or budget for AFACT which is approved by the Los Angeles head office of the MPA. The Court considers that AFACT is, for relevant purposes, the local 'franchise' of the MPA, though with specific additional interaction with Australian entities that are not part of the MPA, such as Village Roadshow and related entities. Nevertheless, it has not been established that AFACT is an agent of the applicants; rather, its position vis-à-vis the applicants is a loose arrangement to provide certain services for the applicants.

AFACT witness – Aaron Guy Herps

83 Mr Herps is the Manager of Digital Affairs of AFACT. Mr Herps has provided evidence of copyright infringing acts of iiNet users. He has sworn four affidavits in these proceedings. The Court accepts the evidence of Mr Herps and no challenge was made to any aspect of it by the respondent.

84 On 3 October 2007 Mr Herps signed up electronically for internet services from the respondent. He selected a 'Home 7' Plan at a cost of $129.95 per month. That is, Mr Herps became a subscriber of the respondent. To access the internet through his account Mr Herps purchased a computer which was connected to the internet via an ethernet cable and an ADSL modem. As far as the Court is aware, Mr Herps continues to be a subscriber of the respondent.

Downloading films and television programs

85 On 27 June 2008 Mr Herps went to the MiniNova website and searched for .torrent files related to various films and television programs of the applicants. He noted that multiple .torrent files often existed for each title that he searched. It was his practice to select the specific .torrent file corresponding to the film which was identified as being the most popular (having the largest number of peers). Mr Herps then used uTorrent to participate in the swarms sharing these files, and by such means he downloaded the files to his computer. When the download was complete he became a seeder and kept the computer operating in the same state and continued to share the files with the swarm.

86 Mr Herps observed that from time to time other peers were downloading pieces from one or more of the files he was sharing with swarms. Such connections were visible to him in

the uTorrent graphical user interface. After completing such process over a period of some months Mr Herps made copies ('images') of his hard drive which were exhibited before the Court. Mr Herps downloaded a total of six films.

87 Mr Herps swore a second affidavit involving a similar process to that described above, in respect of the period from 11 February 2009 until 20 February 2009. However, in this period his method had a crucial difference to the process described previously. During this period, by means of an IP address filter, Mr Herps was able to program uTorrent such that it would only connect to iiNet users. The filter was able to do so, given that, as already discussed, the IP addresses which had been allocated to the respondent (and therefore its subscribers) was publicly available information. After taking this step, Mr Herps repeated the process above of downloading .torrent files from MiniNova which related to films to which the applicants own copyright. The difference of the process enabled Mr Herps to be certain that he would only receive pieces of each film from iiNet users. His affidavit provides evidence of his downloading and sharing of three films in that period.

88 Mr Herps swore a third affidavit in reply to the expert witness of the respondent, Dr Caloyannides. Given that he was not called, no further reference need be made to that affidavit.

89 Mr Herps has also sworn a fourth affidavit in these proceedings which relates to issues of copyright substantiality. As the discussion at [310] and following demonstrates, these issues are irrelevant.

90 Mr Herps' testimony is submitted to be evidence of copyright infringement of iiNet users on two grounds. First, by his direct infringement of the applicants' copyright as a subscriber of the respondent; and second because his evidence recorded connections from other iiNet users who themselves must have been infringing. Whether Mr Herps' actions were infringing will be considered in Part D in relation to the issue of whether he was licensed by the applicants to carry out acts which were copyright in relation to the films.

AFACT witness – Gregory Donald Fraser

91 Mr Fraser is the Operations Manager of AFACT. Mr Fraser undertook the same task referred to by Mr Herps in his second affidavit. Mr Fraser became a subscriber of the

respondent on a 'Home 5' Plan, sought out .torrent files from MiniNova relating to the applicants' films and then proceeded to participate in swarms sharing those films. Like Mr Herps in his second affidavit, Mr Fraser only downloaded pieces of files of the applicants' films from other iiNet users. Mr Fraser was not cross-examined.

92 As with Mr Herps, the applicants rely on Mr Fraser's testimony as evidence of infringement by iiNet users both in the sense that he himself infringed and because he recorded connections from iiNet users who themselves were infringing. Similarly to Mr Herps, whether Mr Fraser was licensed by the applicants will be examined in Part D of this judgment.

AFACT witness – Neil Kevin Gane

93 As mentioned, Mr Gane is the Executive Director of AFACT. Mr Gane has had oversight of AFACT's actions in the gathering of evidence for these proceedings. Mr Herps and Mr Fraser answer to Mr Gane.

Evidence of copyright infringement

94 Mr Gane testified that he was aware from his investigations and his own experience that the scale of copyright infringement of films and television programs taking place on the internet has increased substantially in recent years. He has attached two reports confirming this trend. The first is from a United Kingdom company, Envisional, and the second is from a German company, Ipoque. A report entitled '*Internet Study 2007*' by Ipoque (made between August and September 2007) revealed that in Australia approximately 57% of internet traffic was p2p traffic and 73% of such traffic was associated with the BitTorrent protocol.

95 Mr Gane has also exhibited confidential MPAA reports prepared by Envisional providing an analysis of overall developments related to digital film piracy worldwide. The reports show that the number of persons using the BitTorrent protocol rose steadily over the period assessed and that the BitTorrent protocol remains the most popular p2p file-sharing mechanism.

Investigations of online piracy in Australia

96 From August 2007 AFACT used the services of DtecNet Software APS ('DtecNet') to collect information concerning alleged copyright infringement by internet users in Australia. The contractual arrangement concerning this investigation appears to have been between DtecNet and the Singapore branch of the MPA rather than between AFACT and DtecNet. In June 2008 Mr Gane instructed DtecNet to prepare reports regarding the copyright infringing actions of iiNet users using the BitTorrent system. It would appear that in the period between September 2007 and June 2008, DtecNet investigated 190 Australian ISPs in relation to four different types of file-sharing protocols, including BitTorrent. It then narrowed its investigations to the BitTorrent protocol and targeted four Australian ISPs; namely Optus, Internode, Exetel and the respondent. It was not explained why these particular four ISPs were selected.

97 By email dated 2 July 2008 Mr Gane wrote to the respondent in what would become the first of many 'AFACT Notices'. The email attached a letter which was entitled '*Notice of Infringement of Copyright*'. The letter, addressed to Mr Malone as Managing Director of iiNet relevantly stated:

> AFACT is associated with the Motion Picture Association (MPA), whose members include Buena Vista International Inc, Paramount Picture Corporation, Sony Pictures Releasing International Corporation, Twentieth Century Fox International Corporation, Universal International Films Inc, and Warner Bros. Pictures International…and their affiliates. AFACT represents Australian producers and/or distributors of cinematograph films and television shows, including affiliates of the member companies of the MPA. AFACT's members and their affiliates are either the owners or exclusive licensees of copyright in Australia in the majority of commercially released motion pictures including movies and television shows. AFACT undertakes investigations of infringements of copyright in these movies and television shows.
>
> AFACT is currently investigating infringements of copyright in movies and television shows in Australia by customers of iiNet Limited (iiNet) through the use of the BitTorrent "peer-to-peer" protocol (BitTorrent). Information has been gathered about numerous infringements of copyright in motion pictures and television shows controlled by AFACT's members, or their affiliates, by customers of iiNet (the Identified iiNet Customers). These infringements involve the communication to the public of unauthorised copies of the motion pictures and television shows shared with other internet users via BitTorrent.
>
> Attached is a spreadsheet containing the information relevant to infringing activities of the Identified iiNet Customers occurring between 23 June 2008 and 29 June 2008, including:
>
> a) The date and time infringements of copyright took place;

b) The IP address used by the Identified iiNet Customers at the time of the infringements;

c) The motion pictures and television shows in which copyright has been infringed; and

d) The studio controlling the rights in the relevant motion pictures and television shows.

A CD containing an electronic copy of the spreadsheet is enclosed with the hard copy of this letter.

98 The letter alleged that the spreadsheet attached showed that individual subscribers of the respondent, who were referred to in the AFACT Notice as '*repeat infringers*', were involved in multiple infringements of copyright. The letter stated that AFACT was '*unaware of any action taken by iiNet to prevent infringements of copyright in movies and television shows*'. The letter relevantly continued:

> The failure to take any action to prevent infringements from occurring, in circumstances where iiNet knows that infringements of copyright are being committed by its customers, or would have reason to suspect that infringements are occurring from the volume and type of the activity involved, may constitute authorisation of copyright infringement by iiNet.
>
> AFACT and its members require iiNet to take the following action:
>
> 1. Prevent the Identified iiNet Customers from continuing to infringe copyright in the motion pictures and television shows identified in the spreadsheet, or other motion pictures and television shows controlled in Australia by AFACT's members and their affiliates; and
>
> 2. Take any other action available under iiNet's *Customer Relationship Agreement against the Identified iiNet Customers which is appropriate having regard to their conduct to date.
>
> Please acknowledge receipt of this letter and confirm when the above action has been taken.

99 The letter then attached extracts of the respondent's CRA which had been downloaded from the respondent's website and pursuant to which the respondent provided internet services to its subscribers. The relevant provisions attached to the AFACT Notice were as follows:

> 1. <u>Customer Relationship Agreement (CRA):</u>
>
> **4. USING THE SERVICE**
>
> ***Comply With All Laws***
>
> 4.1 In using the Service, you must comply with all laws and all directions by a Regulatory Authority and reasonable direction by us.

Prohibited Uses

4.2 You must not use, or attempt to use, the Service:

(a) to commit an offence, or to infringe another person's rights;

…

(e) for illegal purpose or practices;

or allow anybody else to do so.

14. CANCELLING OR SUSPENDING THE SERVICE

Cancellation or Suspension By Us

14.2 We may, without liability, immediately cancel, suspend or restrict the supply of the Service to you if:

…

(j) we reasonably suspect fraud or other illegal conduct by you or any other person in connection with the Service;

…

(l) we are required by law or in order to comply with an order, direction or request of a Regulatory Authority, an emergency services organisation or any other authority;

…

(n) providing the Service to you may be illegal; or we anticipate that it may become illegal;

…

(q) there is excessive or unusual usage of the Service;

(r) We are allowed to under another provision of the CRA; or

…

14.3 If we suspend the Service under clause 14.2, the we may later cancel the Service for the same or a different reason.

2. <u>iinet Website</u>

"Copyright Regulations and Illegal Content" from the iinet website located at

(http://www.iinet.com.au/about/compliance/copyright.html), page 2:

NOTE: The hosting or posting of illegal or copyright material using an iinet [sic] service constitutes a breach of iinet [sic] contractual obligation [sic] under the Customer Relationship Agreement Sec 4.1 & Sec 4.2. Such a breach of contract may result in the suspension or termination of service without notice to the subscriber.

100 The spreadsheet attached to the AFACT Notice of 2 July 2008 contained a summary of alleged actions of iiNet users in infringing the copyright of the applicants in the period of 23 June 2008 to 29 June 2008 via the BitTorrent system. The spreadsheet extended over 13 pages of A4 sized paper. It was divided into 11 columns headed '*Peer IP*', '*Date and Time UTC*', '*File Name Downloaded*', '*Hash*', '*Film/TV Title*', '*Studio*', '*% of file Shared*', '*MB Downloaded*', '*% of file Downloaded*', '*Peer Hostname*' and '*Country*'.

101 In addition to being forwarded by email to the respondent, the spreadsheet and letter were also served by hand on the offices of the respondent located in Perth. Attached to the letter was a CD that contained an electronic version of the spreadsheet in the form of a Microsoft Excel file.

102 On 9 July 2008 a further AFACT Notice, in identical terms to that forwarded on 2 July 2008, was sent by Mr Gane to the respondent together with the same attachments as previously, although the spreadsheet was compiled in respect of the period from 30 June 2008 to 6 July 2008.

103 On 16 July 2008 a further letter was forwarded in similar terms. However, this letter also incorporated three DVDs covering the period commencing 23 June 2008 and ending 13 July 2008. These DVDs contained the electronic spreadsheet found on the CD, as well as the underlying data gathered by DtecNet in its investigations. That is, the DVDs contained the packets of data (and therefore pieces of the file) that the 'DtecNet Agent' (see [113] below) received from iiNet users. The DVDs also contained a greater amount of information in relation to each act of infringement alleged. Each included the information under the eleven columns at [100] as well as information entitled '*PeerID*', '*Peer client info*', '*Target Port*' and '*Fingerprint*'.

104 Thereafter AFACT Notices were forwarded weekly to the respondent enclosing the same type of information in similar terms in respect of alleged copyright infringement in the respective week. The respondent does not challenge that in the period of 59 weeks from 23 June 2008 to 9 August 2009, the spreadsheets attached to the AFACT Notices recorded allegations of acts of infringement by the iiNet users. These AFACT Notices, and underlying data attached to them, are the primary evidence before the Court of the actions of iiNet users who are alleged to have infringed the copyright of the applicants.

Expert witness – Nigel John Carson

105 Mr Carson is the Executive Manager of the Forensics Division at Ferrier Hodgson. Mr Carson was engaged as an expert witness for the applicants. His role was to provide two expert reports. The first was a technical investigation and explanation of the BitTorrent protocol and the second analysed the data gathered by DtecNet to verify independently its veracity. Both reports have been exhibited before the Court.

106 The Court found Mr Carson's first report to be of great assistance in developing an understanding of the BitTorrent protocol, and much of its content has been used for the purposes of the technical discussion in Part B of this judgment regarding the BitTorrent protocol.

107 The second report of Mr Carson provided evidence that the DtecNet evidence is reliable, that is, that the underlying data of the AFACT Notices does demonstrate that the packets of data received by the 'DtecNet Agent' (discussed below at [113]) constituted pieces of the films of the applicants downloaded from iiNet users.

108 Mr Carson was a fair-minded and excellent witness. He provided full and forthright answers to all questions asked of him, including those that may not have provided evidence which favoured the applicants. Therefore, the Court considers him to be an impartial witness. The Court accepts the evidence he has provided in this hearing. No challenge was made to his evidence by the respondent, and indeed the respondent actually relies on such evidence.

DtecNet witness – Thomas John Sehested

109 Mr Sehested is the Chief Executive Officer of DtecNet. Mr Sehested gave evidence of the investigation of iiNet users by DtecNet and the collection of data by DtecNet regarding iiNet users which commenced in about June 2008. Mr Sehested confirmed that DtecNet supplied AFACT with Microsoft Excel spreadsheets summarising the data collected from the iiNet users and provided hyperlinks allowing AFACT employees to access a secure FTP server (server allowing the downloading of material by means of the ftp discussed above at [55]) operated by DtecNet which contained the data collected by the DtecNet Agent relating to iiNet users.

DtecNet witness – Kristian Lokkegaard

110 Mr Lokkegaard is the Chief Technology Officer of DtecNet and was responsible for the development of the proprietary software used by DtecNet to gather evidence for the current proceedings. Such software is known as the 'DtecNet Agent'.

111 Mr Lokkegaard provided a confidential report to the Court which contained significant detail concerning the operation of the BitTorrent protocol and the operation of the DtecNet Agent. The Court made an order for confidentiality regarding the report, as was requested. However, a non-confidential version of the report was later exhibited (exhibit SS). The Court will rely on such non-confidential exhibit and Mr Lokkegaard's affidavit (which was not confidential) in explaining the operation of the DtecNet Agent.

112 Mr Lokkegaard swore a second affidavit in reply to Dr Caloyannides. However, as with Mr Herps, as Dr Caloyannides was not called, there is no need to refer to such affidavit further.

Collection of data using DtecNet Agent

113 The DtecNet Agent, being the software used to provide the information underlying the allegations of copyright infringement in the AFACT Notices, is, in essence, a BitTorrent client. However, it has been programmed to fulfil specific functions beyond that of a publicly available BitTorrent client, such as Vuze or uTorrent. The process by which the DtecNet Agent operated was as follows:

a) An employee of DtecNet would identify .torrent files of interest based on content files which were supplied by the applicants/AFACT. The DtecNet Agent would then open the .torrent file.

b) By opening the .torrent file the DtecNet Agent, like any BitTorrent client, was able to query the tracker; connect to peers in the swarm; and download pieces from those peers. Given that DtecNet was gathering evidence of iiNet users infringing, the DtecNet Agent employed an IP filter similar to that used by Mr Herps and Mr Fraser to ensure that it only connected to iiNet users. Initially, the DtecNet Agent downloaded one complete copy of the film sought to be investigated. This copy was then viewed to

ensure that the film corresponded with one that was owned by the applicants. Given the information already discussed regarding hashes, this process established beyond doubt that a particular file hash corresponded with a film of the applicants.

c) The DtecNet Agent then reconnected to iiNet users who had a copy of the file or parts of the file of interest and downloaded a piece of that file from those users. It then matched the piece downloaded with the piece hash through the hash checking process discussed in Part B. The DtecNet Agent then recorded information referrable to the peer from which it had downloaded that piece of the file. The DtecNet Agent was calibrated to download only one piece from each IP address and then disconnect from that IP address. It was set up to download a new piece from the same IP address every 24 hours.

d) The DtecNet Agent was designed to create a running log of every activity and this included every single request sent between computers and every packet of data exchanged between those computers. Accordingly, every aspect of the connection and download was recorded and logged by the DtecNet Agent.

e) All the information received or logged by the DtecNet Agent was recorded and stored securely on DtecNet's servers. The servers were located in Copenhagen under Mr Lokkegaard's supervision.

f) Once recorded in DtecNet's secure server, a DtecNet employee prepared a report containing some or all of the information recorded by the DtecNet Agent and incorporated that information into a Microsoft Excel spreadsheet which was provided to AFACT.

Mr Lokkegaard stated that the data collection process carried out by the DtecNet Agent is highly accurate and reliable and is based on a confirmed connection and receipt of a piece of the file from a remote computer. As mentioned, the second report of Mr Carson independently verified such method.

Michael John Williams

114 Mr Williams, solicitor for the applicants, provided numerous affidavits in these proceedings. His primary role was to collate evidence before the Court by means of the AFACT Notices and also, following discovery from the respondent, to highlight particular aspects of the evidence of infringements as detailed hereunder.

'Repeat infringer bundles'

115 Exhibits MJW-1 and MJW-8 are spreadsheets that collate data from the information attached to the AFACT Notices by means of the 'PeerID'. The PeerID is a number generated by the BitTorrent client upon the program initiating and it remains until the BitTorrent client is closed. As mentioned, the PeerID data was not included in the spreadsheets attached to the AFACT Notices. Rather, it was to be found in the DVDs attached to the AFACT Notices. This number is broadcast to the swarm, and thereby the PeerID of other peers in the swarm can be ascertained. As will be explained in more detail in Part D at [277]-[278], the PeerID is evidence of one computer involved in the infringement of a film or multiple films over a period of time. There was some cross-examination of Mr Williams on the question of the factors necessary to constitute repeat infringement. The Court finds that the definition of repeat infringement is a legal issue, and thus the opinions of any witnesses are irrelevant. The Court's finding on such issue is found in Part D of this judgment.

Bundles involving the RC-20 accounts

116 As will be explained in more detail at [122] and following below, during the process of discovery the respondent was ordered to provide data to the applicants in relation to 20 accounts of its subscribers (as described hereunder, these are referred to as the 'RC-20 accounts'). Exhibits MJW-10, MJW-13, MJW-15 are each bundles which contain this data. MJW-15 is the entire history of communications, whether by telephone or email, between the respondent and each subscriber account. MJW-13 is the login/logout history and history of allocation of IP addresses to those 20 accounts over a period of time commencing with the first AFACT Notice. Finally, MJW-10 uses the IP history in MJW-13, taken in conjunction with the DtecNet evidence in the AFACT Notices, to produce spreadsheets of the alleged infringements that have occurred in relation to each of the 20 subscriber accounts.

117 Mr Williams was cross-examined particularly in relation to MJW-10. While the respondent was able to identify some anomalies in the generation of the spreadsheet, particularly in that some individual allegations of infringement appear to duplicate others in terms of time, as will become apparent from the Court's discussion of the primary infringement issue in Part D below, these issues are an irrelevancy. Despite these anomalies, the Court finds that, on the whole, MJW-10 is reliable.

DNS Lookups

118 Exhibit MJW-17 was created using a similar process as MJW-1 and MJW-8. However, rather than arranging the DtecNet data by means of the PeerID, MJW-17 organises the DtecNet data by means of the '*Peer Hostname*' column. This is used to demonstrate that one peer hostname was responsible for multiple infringements.

119 The purpose of the exhibit and affidavit which attached it appears to be to demonstrate that it is possible to gather details from publicly available sources of information in relation to a static IP address, such that it can be known who is using a particular IP address and therefore, who is potentially infringing copyright. As mentioned, most accounts with the respondent have dynamic IP addresses allocated to them, but as already mentioned, it is possible to receive a static IP address for specific purposes, such as commercial enterprise.

120 The process by which this information is sought is by means of a reverse DNS lookup. 'DNS' stands for 'domain name service'. Whenever one types a URL such as http://www.google.com into a web browser one is actually typing what is known as a 'domain name'. As already explained, computers communicate in the IP protocol by means of IP addresses. However, IP addresses are very difficult for people to remember. Domain names essentially render IP addresses in a form that is easy to remember. So, when one seeks out http://www.google.com, one is actually seeking out the IP address(es) associated with Google's website. In order for a computer to actually connect to Google's servers the domain name must be converted into an IP address. This occurs by means of a DNS lookup. This information, linking domain name to IP address, is stored in various servers around the world. The evidence of Mr Malone and Mr Carson establishes that this information is regularly updated, as it is crucial to communication over the internet.

121 However, the reverse is also possible, that is, it is possible to take an IP address and find a domain name. This information is not as crucial to the operation of the internet and thus it is less regularly updated. It was this information which was used to prepare the affidavit of Mr Williams and exhibit MJW-17. An affidavit sworn by Mr Malone suggests that the information relied upon by Mr Williams in preparing his affidavit on this issue was unreliable, and both Mr Carson and Mr Lokkegaard independently confirmed that reverse DNS lookups were not always reliable. Consequently, the Court finds that MJW-17, and the affidavit of Mr Williams attaching it, are unreliable and the Court will not rely on them. It does not appear that the applicants chose to make any particular submissions in closing in relation to MJW-17 and the corresponding affidavit.

The iiNet subscriber accounts

122 During the course of the discovery process the applicants sought information concerning some subscribers of the respondent to enable the information relating to those accounts to be matched with the DtecNet evidence. On 15 June 2009 the Court made an order allowing the applicants to select a number of IP addresses and times as logged by the DtecNet Agent in its investigations, as well as some identified by Mr Herps and Mr Fraser from their investigations. This data was then provided to the respondent who examined the IP addresses and times provided in order to identify from them 20 unique subscriber accounts.

123 This process of matching IP address and time to a subscriber account is one of the key evidentiary issues in these proceedings, and it is dealt with in relation to the Telco Act defence in Part E2 of this judgment. ISPs generally keep records of those IP addresses that are associated with subscriber accounts at any given time. Thus, by knowing an IP address and time, a link can be made to a subscriber account, thereby identifying the account subscriber.

124 As it transpired, 45 IP addresses and times were needed to generate 20 unique subscriber accounts. This resulted from the fact that some IP addresses and times related to the same subscriber accounts (remembering that as IP addresses are assigned dynamically it is possible for one subscriber account to have multiple IP addresses over time). These subscriber accounts (the 'RC-20 accounts') are the most specific evidence of copyright infringement by iiNet users in these proceedings. In relation to each account, for the period

from 1 July 2008, the respondent provided evidence of the allocation of IP addresses, login/logout details, time spent online and disconnection reasons. The respondent also provided all correspondence between the respondent and those subscriber accounts from 1 July 2008 to August 2009. The Court ordered that any personal information related to these accounts be redacted, such that it was impossible to link the data to any particular persons during these proceedings. The Court considered that it was appropriate for such information to remain confidential given that the subscribers of those accounts were not parties to these proceedings.

125 As already discussed, this evidence has been compared with the DtecNet evidence in MJW-10 to create a list of alleged infringements occurring on those accounts. Specific factual issues arising from such evidence will be addressed from time to time throughout the judgment.

Studio witnesses

126 Each of the applicants have called witnesses ('studio witnesses') to confirm matters such as their ownership or exclusive licence of the identified films, the subsistence of copyright in such films and the absence of licence to any iiNet users to do the acts comprised in the copyright of the films.

127 Mr Phillipson testified for Village Roadshow and its related companies. Mr Wheeler testified for 20th Century Fox and related companies. Mr Perry provided evidence regarding Paramount and its associated or related companies. Ms Solmon provided evidence regarding Columbia Pictures and related companies. Ms Reed provided evidence regarding Disney and its affiliated companies. Ms Garver testified on behalf of Universal and its numerous associated companies. Mr Kaplan testified for Warner Bros and related entities.

128 The studio witnesses were forthright in their evidence, and the Court found them to be reliable witnesses. The primary controversy arising during their cross-examination was their ability to provide evidence upon the question whether the AFACT investigators, Mr Herps and Mr Fraser, were licensed by the applicants to download the applicants' films using their iiNet accounts. As will be apparent from the Court's discussion in Part D of this judgment,

though the Court finds the studio witnesses to be reliable, their evidence is not necessarily conclusive on this issue.

Respondent's witness – Michael Martin Malone

129 Mr Malone is the Managing Director and Chief Executive Officer of the respondent. His key responsibilities are related to customer service; the financial performance of the respondent; business planning and strategy; and corporate governance.

130 The undertaking of the respondent is substantial. As indicated, there are approximately 490,000 subscribers subscribing to the respondent and related entities, making it the third largest ISP in Australia. It operates call centres in Perth, Sydney, Auckland and Cape Town. There are approximately 600 customer service representatives in the respondent's employ.

131 Mr Malone provided extensive evidence which will be referred to from time to time throughout the judgment. A key issue for present purposes is his credit as a witness.

Findings as to the credit of Mr Malone

132 The applicants have mounted a vigorous challenge to the credibility of Mr Malone, asserting that he was neither a truthful nor reliable witness. It has been submitted that the Court should not rely on his evidence except where it is against his interests or it is independently corroborated. It is submitted that Mr Malone was determined to advocate the respondent's cause at every opportunity and where he sensed a conflict between that cause and the truth, he was prepared to subordinate the latter in favour of the former.

133 The Court rejects the attack on the credit of Mr Malone. Mr Malone was an impressive witness who remained consistent (for the most part) in the evidence he gave during three days of gruelling and unnecessarily hostile cross-examination. The specific submissions made by the applicants will be addressed below. However, even in the circumstance that the Court finds against Mr Malone in relation to certain evidence he provided on specific issues, such findings do not lead the Court to make a generalised finding that he was an unreliable witness.

134 In so far as it is alleged that Mr Malone found it impossible to disassociate himself from the respondent's 'cause', such a generalised allegation cannot be sustained. Certainly Mr Malone gave evidence supportive of the respondent's position and this position was at odds with the applicants' position, but the Court is not able to infer that in providing those answers they were not provided honestly, nor that they were necessarily wrong. Mr Malone's demeanour was of someone who believed what he was saying without reservation. Whether Mr Malone's beliefs in relation to the law and the respondent's legal obligations were accurate is a distinct matter from whether he provided evidence of that which he honestly believed. Mr Malone may not have been a helpful witness to the applicants' counsel, but that did not render Mr Malone an unhelpful witness to the Court. Mr Malone was occasionally asked questions which were technically imprecise and thus potentially misleading. His refusal to concede matters, his desire to seek clarification and his careful answers were not obfuscation as was submitted, but rather seemed to represent Mr Malone's desire to be accurate in the evidence he provided to the Court and his refusal to be forced, by the manner of questioning, into giving evidence that he did not believe to be correct.

135 The Court rejects the submission that Mr Malone '*like iiNet itself, has been compromised by his extreme views on the role and responsibilities of an ISP*'. Merely because the views expressed by Mr Malone did not accord with the interests of the applicants does not render those views '*extreme*'. The flaw in the applicants' submissions relating to the credit of Mr Malone is that they proceed on an assumption that the applicants have already succeeded in these proceedings; that the respondent has been found to have authorised copyright infringement; and that therefore resisting the applicants' assertions, or refusing to co-operate with the applicants, inevitably leads to the result that Mr Malone's opinions must be '*extreme*'. Such posture tended to convolute these proceedings. The purpose of these proceedings is to decide whether the respondent authorised. Mr Malone might be found to be wrong in his views, but that does not make his views or position, per se, '*extreme*'.

136 There were four specific issues, considered in detail hereunder, that the applicants submitted weighed against Mr Malone's credit. The first was his actions in respect of the Westnet policy, the second his evidence regarding the respondent's repeat infringer policy, the third his view as to whether the Telco Act prohibited the respondent from acting on the

AFACT Notices, and finally various statements made by him which suggested that he had a disdainful or contemptuous attitude towards the interests of the applicants.

WESTNET ISSUE

137 Westnet was an ISP that was acquired by the respondent on or about 8 May 2008. Westnet had a policy of passing on copyright infringement notifications to its subscribers. It is important to observe, for reasons discussed later, that such notifications were not AFACT Notices and that they differed from AFACT Notices in important respects. Substantial submissions have been made by the applicants on the issue of the Westnet policy.

138 Mr Malone learnt from Mr Bader (the Chief Technology Officer of the respondent) on or about 17 September 2008 that Westnet had received an email alleging copyright infringement which had been forwarded on to a Westnet subscriber. Mr Malone then learnt from the Chief Operations Manager of Westnet, Mr Cain, that in sending the notice to the subscriber no response was being sought. Rather, '*it is merely a heads up*' from which the Court infers that Westnet was merely passing on allegations of infringement. This was confirmed by Mr Cain's comment that '*no notes, flags or records are kept on the customer's account in relation to the notices and no further action (beyond forwarding the email) is taken*'.

139 On 30 October 2008 Mr Malone raised with Mr Cain and Mr Ariti (the Chief Information Officer of the respondent) the question of Westnet's practice in respect of AFACT Notices. The Court accepts that when Mr Malone referred in his evidence to AFACT Notices, he was in fact referring to copyright infringement notices generally, not the AFACT ones, since AFACT chose not to specifically investigate Westnet (see discussion at [96] above).

140 The Court finds that Mr Malone was unaware of the policy of Westnet prior to September 2008, and that he did not inquire, nor subsequently learn, precisely how long it had been in operation. Despite being asked, on the Court's count, no fewer than 30 times in multiple different ways, Mr Malone refused to alter his answer that he did not know how long the Westnet policy had existed for, only that he knew that it existed from September 2008 when he was first made aware of it. While he could accept that it was likely that the Westnet

policy existed before he found out about it in September, as he said, that did not mean he *knew* it existed before that date. The Court accepts Mr Malone's answers.

141 There is no evidence before the Court of the period during which the Westnet policy operated. The Court does not believe that the email exchange tendered on the issue provides sufficient evidence to draw the conclusion that the policy was in existence from 2006 as was submitted. The email chain on 17 September 2008 contains a sample notification to certain subscribers alleging copyright infringement from 2006 from the '*WestnetWiki*' (a database Westnet used for training purposes) on the topic of '*Infringement Notices*'. That establishes that Westnet had been receiving allegations of copyright infringement from at least 2006. However, it does not follow from that evidence alone that Westnet had a policy of passing those notifications to its subscribers from 2006. The Court accepts that the Westnet policy was in place at least as at September 2008 when Mr Malone first became aware of it, but can make no finding as to how long it had existed prior to that date.

142 The chain of emails demonstrates that Mr Malone discovered that Westnet had a practice of passing on copyright notices to its subscribers who had allegedly infringed, a practice which was inconsistent with the respondent's policy. In internal emails, Mr Malone described such policy as doing '*damage to the industry and damage to iinet's [sic] position*'. The Court does not accept the applicants' submission that these statements bear adversely upon Mr Malone's credibility. It cannot be doubted that Mr Malone did not agree with the applicants' view of the appropriate treatment for notices of infringement, but that does not render Mr Malone dishonest. His evidence is consistent with his honestly held opinion.

143 Mr Malone explained that he considered the practice of Westnet damaging because the '*industry was in negotiations with MIPI, ARIA and AFACT*' in respect of copyright infringement, and Westnet's policy was inconsistent with the position of the internet industry more broadly, as well as being inconsistent with the respondent's policy on the issue.

144 The Court accepts that Mr Malone considered it inappropriate and even unworkable to have different practices relating to infringement notices within the respondent's business and it was for this reason alone that he ended the Westnet policy. As Mr Malone said:

> …we took over Westnet in May…that meant hundreds of policies and ways of approaching business were changed over the following few months. This was one of

> them. I was forever regularly tripping over policies where there were slight differences in the way that Westnet operated and the way iiNet operated…In each case, when I saw a policy that was not operating the same, I said, guys, you need to operate under the iiNet policy from this point forward.

145 These events occurred prior to 20 November 2008, being the date on which these proceedings were commenced. Accordingly, it could not be said, as implied by the applicants, that it was the institution of these proceedings which led the respondent to the change Westnet's policy. The Court accepts that Mr Malone was motivated to bring an end to the Westnet policy to ensure consistency within the business of the respondent, not because it was embarrassing for the purposes of these proceedings.

146 The applicants also attack Mr Malone's credit arising from his estimation provided in an answer during cross-examination that Westnet's policy of passing on notifications '*only applied to a small percentage of notices*'. The applicants submitted that such answer was not based on fact and was an example of Mr Malone's willingness to state as a fact something of which he had no direct knowledge in support of the respondent's position.

147 When such answer was challenged, Mr Malone readily acknowledged that he had no personal knowledge of the proportion of notifications passed on to Westnet's subscribers. He stated that he was making an assumption or an estimate. He stated '*I know it was not the complete form of all the notices and I know that Westnet wasn't receiving any AFACT notices*'. He later stated that he '*actually believed it to be a small percentage*', but acknowledged that he did not have any '*direct evidence that it is a small or large percentage*'.

148 The Court finds that it was Mr Malone's belief that only a small number of notices were passed on, but, as he correctly acknowledged, he could not point to any specific evidence that this was in fact the case. It may well have been an impression formed by Mr Malone from his discussions with Mr Cain or Mr Ariti on the issue. The Court is unable to make any finding as to the proportion of such notices passed on to Westnet subscribers, and is not prepared to find that Mr Malone's answer indicated dishonesty.

149 As a further issue, the applicants submit that Mr Malone's claim that the passing on of warning notices to the respondent's subscribers would be onerous was obfuscation. The

applicants attack Mr Malone, claiming that when swearing his second affidavit he should have mentioned that Westnet had a policy of passing on notifications to its subscribers. It is submitted that Mr Malone was less than truthful in his claim that it would constitute a very substantial burden for the respondent to have to pass on notices to its subscribers given that he did not mention Westnet's policy in such affidavit, or make enquiries concerning the practicality of such steps.

150 The Court does not accept that this issue bears on Mr Malone's credibility. As he said in his cross-examination, the policy to which he was referring to in his second affidavit was a policy of warning and termination of subscribers, being a more complicated procedure than a policy of merely passing on notifications of infringement, as had been Westnet's practice.

151 As already explained, and as explained by Mr Malone, Westnet's policy was to pass on notices to subscribers and nothing more. Westnet had no intention to act on those notices by terminating subscribers, and never did so: see [138]. Consequently, Westnet's policy was a more narrow policy than that which Mr Malone understood AFACT to be seeking, namely prevention of copyright infringement by notification and ultimately by disconnection of subscriber accounts. Mr Malone was under no obligation to mention Westnet's policy in his second affidavit.

152 As to the more narrow issue of the technical feasibility of passing on notices, it may have been prudent for Mr Malone on reflection to have consulted those who had implemented Westnet's policy concerning the cost and feasibility of passing on notifications. However, Mr Malone provided evidence that he had enquired of technical staff and drew upon his own knowledge from his background as a computer programmer in preparing such affidavit and that this was sufficient to provide the essential evidence.

153 Further, the AFACT Notifications, as the applicants are want to remind the Court, are far more detailed and thus different from the 'robot' notices (discussed below at [192]) which were the type of notices passed on by Westnet. Consequently, the mere fact that Westnet had implemented a system to forward robot notices to subscribers may not have been at all relevant to the technical feasibility of forwarding AFACT Notices, or the allegations and information contained therein.

154 For all these reasons, the Court rejects the applicants' submissions regarding the Westnet policy, both as to its relevance to Mr Malone's credit, and as to its broader relevance to these proceedings.

REPEAT INFRINGER POLICY

155 The applicants submitted that the respondent had no repeat infringer policy, and that Mr Malone's testimony to the contrary demonstrated that he was simply untruthful. The issue of the repeat infringer policy is discussed in detail in Part F of this decision.

156 There has been no detailed Australian judicial consideration relating to the requirements of a 'repeat infringer policy' in respect of category A activities for the purposes of Division 2AA of Part V of the Copyright Act. The Copyright Act is silent, giving no indication of any requirements for such policy. Consequently, there is no guidance in respect of the interpretation of such term. Yet the cross-examination of Mr Malone on the issue proceeded essentially upon the basis that there could only be one type of repeat infringer policy, being the policy sought by the applicants (warning and termination). The applicants submitted that because Mr Malone did not have this policy, and because there was no written policy, he was misleading the Court concerning the existence of any policy.

157 Mr Malone's evidence acknowledged that was there was no written policy (as distinct from written material which evidenced the policy). However, he and Mr Dalby (the Chief Regulatory Officer of the respondent: see [193]) were aware of the outline of a procedure or policy, which the respondent had formulated, namely that if a Court ordered a subscriber account be terminated or if a Court found that a subscriber of the respondent infringed copyright or a subscriber admitted infringement, the respondent would terminate that subscriber's account. When Mr Malone explained that no one had been terminated because no one had been found to infringe copyright he was asked whether this was some kind of '*joke*'.

158 It is the Court's prerogative to decide whether the respondent had a repeat infringer policy of the kind referred to in the Copyright Act. It should not be assumed that the respondent did not have a policy and that consequently Mr Malone was untruthful. The Court observes that this subject matter was a prime example of the intemperate cross-examination of Mr Malone. The respondent's policy was not a joke, and its conduct was entirely

consistent with the policy as outlined even though it may not have been the kind of policy that the applicants anticipated. As will be explained in more detail in Part F, since there are no statutory requirements for a 'repeat infringer policy', the Court concludes that the respondent's policy as described by Mr Malone was sufficient to constitute a policy for the purposes of the Copyright Act. It is no less so merely because the respondent's policy was one which was not envisaged by the applicants. The Court rejects the applicants' suggestion that Mr Malone's testimony on this issue bears upon his credit.

TELCO ACT DEFENCE

159 The applicants submitted that since the evidence demonstrates that the provisions of the Telco Act were not initially considered by the respondent as an obstacle preventing compliance with the AFACT Notices, the raising of such issue reflects adversely upon Mr Malone's credit. The applicants assert that such issue was apparently not considered by Mr Malone nor by Mr Dalby as a genuine prohibition on the respondent complying with the AFACT Notices.

160 Whilst questions were asked of Mr Malone in cross-examination concerning his belief that the Telco Act operated to prohibit the respondent complying with the AFACT Notices ('the Telco Act defence'), no questions were put to him upon the question whether he discussed with Mr Dalby the Telco Act defence, and similarly Mr Dalby was not cross-examined on the question whether he had discussed such defence with Mr Malone. The Court accepts the submissions of the respondent that in such circumstances it is unfair to make allegations against Mr Malone's credit based upon the fact that Mr Dalby in his evidence in chief did not refer to the Telco Act defence.

161 The Court finds that Mr Malone genuinely believed that the Telco Act stood in the way of compliance with the AFACT Notices though it is unclear when such belief arose. This does not mean that his understanding is correct, it merely means he *thought* it was. Not being a lawyer, it was unlikely that Mr Malone would have appreciated the intricacies *why* the Telco Act stood in the way, merely that it did. Consequently, while it could certainly be pointed out, as it was pointed out to Mr Malone in cross-examination, that there were inconsistencies in his actions and the Telco Act defence, it may not have been apparent to Mr

Malone that this was the case. An inconsistency to a lawyer is not necessarily an inconsistency to a lay person.

162 Even if the Court be wrong in its conclusion on this issue, the mere fact that there were inconsistencies in Mr Malone's actions and his comprehension of the consequences of the Telco Act are insufficient to make a broad finding as to his honesty and credit.

VARIOUS OTHER STATEMENTS OF MR MALONE

163 The applicants relied upon certain statements, taken in isolation, as indicative of Mr Malone's credit. An example is Mr Malone's characterisation of the respondent's policy compared to Westnet's policy as being '*a little less umm proactive*'. The applicants also allege that Mr Malone demonstrated a contemptuous attitude towards the applicants when he said, in answer to a question whether the respondent's approach towards protecting copyright was to be obstructive, '*[w]e are not standing in the way of you [the applicants] taking any action whatsoever, of copyright holders taking action whatsoever*'.

164 The Court is unable to draw any inference of dishonesty or obstructionism by Mr Malone from either of the above statements. Mr Malone was consistent in his evidence throughout his cross-examination that in his opinion the task of policing copyright infringements remained the responsibility of the applicants, and that they were not entitled to transfer such responsibility to the respondent. This consistency is evidence of honesty, not dishonesty. Even if the Court had concluded otherwise it would not have rendered Mr Malone an untruthful witness because of his expressed beliefs.

165 As a further basis for attacking Mr Malone's credit, the applicants submit that an adverse finding should be made against him because of his stated refusal to act upon notices from '*Jo Blow*', which is clearly a reference to a third party. The applicants submit that they, being the major film studios, could not possibly be considered '*Jo Blow*' when copyright infringement of their films is under consideration.

166 The Court treats such casual remark as being no more than an expression of Mr Malone's consistently stated position, namely that the respondent would not act upon unsubstantiated complaints. Despite the applicants' attempt to equate Mr Malone's statement

about '*Jo Blow*' as being indicative of disdain for copyright owners, that is, the applicants, it must be remembered that the applicants were not the entities making the allegations of copyright infringement in the lead up to these proceedings: rather, AFACT was doing so. As has been discussed above at [80]-[82], and will also be discussed below at [629], the exact relationship between AFACT and the actual copyright owners (the applicants) is, at best, unclear. The Court rejects the applicants' submission.

PROSECUTION OF MR HERPS

167 When the respondent first became aware that Mr Herps had opened an account with it and was deliberately using its internet service for the sole purpose of downloading the applicants' films, Mr Malone, in an internal email, suggested that Mr Herps should be prosecuted.

168 The applicants submit that an adverse inference of credit should be drawn against Mr Malone given such email or arising from Mr Malone's answers to the issue in cross-examination.

169 From the perspective of a lay person with some understanding of copyright law, it might have been concluded that Mr Herps committed a crime because of his deliberate breach of copyright. Mr Malone was obviously aware that it was possible for copyright infringement to be a crime as well as a statutory tort. Ultimately, as will be made clear in Part D, Mr Herps committed no crime and no tort because he did not infringe copyright.

170 Further, it is not clear that Mr Malone was speaking other than tongue-in-cheek when he made the suggestion, and a similar observation might be made in relation to Ms Moonen's (the respondent's compliance officer) subsequent email to Detective Sergeant Taylor of the Western Australian Police Force on 21 November 2008 which stated:

> Hey Duncan,
>
> We'd like to report the client who "posed" as an iiNet customer, downloaded a whole pile of content, and then is now suing us as he was able to infringe copyright.
>
> Is there any way I could call in a personal favor [sic] and have that individual prosecuted? Today?
>
> :)

The Court believes that the '*:)*' following the email indicated that it was not intended to be to be taken seriously. Though it might perhaps suggest an overly close relationship between the respondent and the police, there is no basis upon which the Court can draw any adverse credit inference against Mr Malone arising out of this incident.

171 As an aside, the Court notes that AFACT, the organisation which the applicants use to aid in enforcement of their copyright, itself blurs the distinction between tortuous copyright infringement and criminal acts involving copyright, as seen in its name: Australian Federation Against Copyright *Theft* [emphasis added].

'Compelling evidence'

172 During his answers in cross-examination concerning the content of the AFACT Notices, Mr Malone stated that he considered the AFACT Notices to be '*compelling evidence*'. The applicants seized upon such term to found a submission as to Mr Malone's credibility as well as to support their claims.

173 The issue is relevant and relied upon by the applicants for a variety of reasons. The applicants submit that it would be inconsistent for Mr Malone to maintain that he believed that the AFACT Notices were compelling evidence of infringements carried out by iiNet users, yet claim simultaneously that the AFACT Notices were mere allegations and thus they could not be acted upon by the respondent. This issue is relevant to the respondent's knowledge of infringements which, in turn, is a matter relevant to authorisation.

174 On 13 December 2008 (that is, following the commencement of the trial) Mr Malone made a comment ('post') on an online forum at http://www.whirlpool.net.au ('Whirlpool forum'). Mr Malone relevantly said within that post:

> With the evidence that AFACT has, I'm betting that a magistrate will happily issue an order for us to disclose the account holder's identity for under $50. AFACT can then directly contact the customer, warn them, raid them, or sue them. Whatever the action, it will then be overseen by the independent legal system.

175 Mr Malone was then cross-examined on this post and the first mention of '*compelling evidence*' then occurred:

> Certainly by that date you were satisfied that AFACT had evidence of infringing

> activity by – on your customer accounts?---Yes, we had been provided with them.
>
> Evidence which you thought proved it?---I thought evidence which was compelling and ought to be tested.
>
> Compelling evidence, correct?---What was being alleged there was that customers did something at this time. I didn't know what your collection methods – sorry, I say "you" but I didn't know what AFACTs collection methods were, but believed that they should be reviewed by an independent third party to take them to the next step.

176 Two issues arise from this exchange. Firstly, it is unclear from this exchange whether Mr Malone accepted the reliability of the method of collection of the evidence at face value, or whether he found it convincing but could not be sure of its reliability in light of the fact that it had not been found by a Court to be convincing. The word '*compelling*', according to the Oxford Dictionary, means '*demanding attention, respect*'. '*[C]ompelling*' does not mean 'conclusive'. Having said this, Mr Malone did not explain what he meant by such term.

177 Another issue is *when* it was that Mr Malone first formed this opinion:

> And you describe that as compelling evidence?---Yes.
>
> So you regarded the notices you received as compelling evidence; correct?---This is post litigation being commenced.
>
> Well, it was 13 December?---Yes.
>
> And I think you have indicated the evidence you are referring to was the evidence consisting at that stage simply of the notices?---Yes.

Later Mr Malone said:

> Do you want to resile from your use of that expression?---No, I have now since these proceedings have commenced, I have been allowed to see what the DtecNet has done, and how it is collected, and I think it is very different from what was done in the past.

The reference to '*in the past*' would appear to be a reference to investigations conducted in previous years by Media Sentry, a company that made allegations of infringement using a different evidence gathering mechanism to DtecNet prior to the service of any AFACT Notices.

178 Such evidence makes it difficult to discern at which point in time Mr Malone formed the view that the DtecNet evidence was '*compelling*'. There is no evidence that Mr Malone formed such opinion on first receipt of the AFACT Notices. However, it would appear that he had formed such opinion by December 2008, prior to the receipt of the affidavit of Mr

Lokkegaard specifying the DtecNet Agent's method, which was filed on 25 February 2009. Therefore, the Court does not believe the last statement in [177] qualifies the earlier statements. However, the more important question is what Mr Malone meant by '*compelling evidence*'.

179 The Court believes it is important that the phrase '*compelling evidence*' was used in the context of a discussion of the use of such evidence before a Court, or in the context of verification of that material, such as obtaining preliminary discovery. Implicit in both scenarios is the necessity that it be verified by an independent review of the evidence. Such interpretation flows from Mr Malone's qualification that '*compelling evidence*', as he said, '*should be reviewed by an independent third party to take them to the next step*' because '*I didn't know what [AFACT's] collection methods [were]'*. Mr Malone's position was therefore clearly stated. That is, he considered that the material, admitted as evidence, might persuade a court of its veracity, but such possibility did not result in the dispensation of that court ruling. Indeed, all of Mr Malone's evidence on this issue was consistent, namely that it is for an independent third party, such as the Court, to deal with the allegations of infringement, to establish their truth. Mr Malone's position is exemplified by the following evidence:

> Well, the examination they undertook was before the commencement of the proceedings, wasn't it?---Between July and December we did revert back to AFACT at the point in July and several times afterwards, to say that what you have got here appears to be legitimate from what you are showing to us. Why don't we go off to a court now, or to the police and get something done about this. As I say in here, we couldn't jump from allegation to punishment. We don't have the judicial ability to do that.
>
> …
>
> You assessed it at the time, that is, at a time prior to December, as compelling evidence, didn't you?---It's evidence of incidents that were observed by AFACTs investigators, and that they claimed they observed. If that was taken to a court and said, here is what we saw, and subjected to a third party review, I was and still remain of the view that the court would be quite happy to let you take direct action against the clients.
>
> …
>
> And that was based, I suggest to you, on an assessment undertaken by Mr Parkinson and Mr Dalby and reported to you?---No. I have been seeing these notices for over a decade. I know what's being alleged in here. It's an allegation of something occurred at this time and this place. My view is then I didn't observe that occurring. I have no way of assessing if it was true or not. The only person that can verify if it was true was your own investigator, therefore your own investigator should take their

evidence which is compelling and take it off to someone else for a third party review.

180 At most, the Court considers that Mr Malone's reference to '*compelling evidence*', read in the context in which the words were used, is evidence that Mr Malone accepted that the AFACT Notices established the likelihood that the conduct being alleged was occurring; that he formed such opinion in December 2008; but that nevertheless he remained steadfastly of the belief that until such material was validated by a court the respondent had no sound basis for proceeding upon it against any subscriber. Mr Malone never suggested that the AFACT Notices provided conclusive evidence of infringements.

Freezone

181 Mr Malone provided evidence of a service that the respondent offers to its subscribers known as Freezone. When a person becomes a subscriber of the respondent, that person does so pursuant a particular plan. Each plan allocates a monthly 'quota'. This quota, measured in gigabytes, is the amount per month that the subscriber can download on that account (subject to 'shaping'). Generally speaking, the more costly the plan, the greater the allocation of quota per month.

182 When an iiNet user exceeds this quota they are 'shaped' which means the speed of their connection is slowed to reduce their ability to download because the process of downloading data takes longer. Mr Malone deposed that the respondent was the first ISP in Australia to introduce 'shaping' to control excessive downloading instead of imposing excess usage charges, whereby any downloads over quota would incur a fee per megabyte.

183 However, any data downloaded from the Freezone is not included in the monthly quota of a subscriber. In this sense, an iiNet user can consume unlimited amounts of data from the Freezone per month. Further, an iiNet user is still able to use as much data at maximum speed as is desired per month in the Freezone, even if that subscriber is otherwise shaped for that month.

184 The respondent has made a number of agreements with various content providers to make their content available on the Freezone. For example, the respondent has made an agreement with Apple iTunes, a major business in the online distribution of media such as music, television programs and films. If an iiNet user buys a television program on iTunes,

that television program must be downloaded. It will usually be some hundreds of megabytes which would otherwise count towards monthly quota. Given that the most popular 'Home' plan of the respondent is 'Home 2' unbundled, which allocates a monthly quota of two gigabytes, it is easy to see that if downloads of iTunes television programs contributed towards quota, the subscriber would not be able to download many programs before reaching the quota and thus having their downloading speed reduced by shaping. The evidence of Mr Dalby demonstrates that, at the time of swearing his affidavit, 38 of the 86 identified films (which includes television programs) were available from iTunes. A significant amount of content appears to be consumed by iiNet users through iTunes. By way of example, on 23 June 2008 49,637 iiNet subscribers downloaded content from iTunes through Freezone.

185 The respondent has also made an agreement with the ABC and its iView website, which allows people to watch ABC programs of their choice online when they choose to, rather than having to watch ABC1, ABC2 or ABC3 in accordance with the scheduling of the network. Unlike iTunes, the television programs on iView are not downloaded: rather they are 'streamed' which means that, once watched, the program does not remain on the computer. However, whether content is downloaded or streamed, it will still count as use of quota unless it is in the Freezone. Similarly to iTunes, television programs on iView will be many hundreds of megabytes which could easily cause a viewer to reach their monthly quota. The provision of Freezone essentially allows unlimited viewing of ABC television content for iiNet users.

186 These examples are not the only content available on Freezone, but the Court considers that they are the most important content available on Freezone for the purposes of these proceedings. It would appear from the evidence of Mr Buckingham (the Chief Financial Officer of the respondent: see [221]) that Freezone is provided to the respondent's subscribers as a net expense for the respondent. However, as submitted by the applicants, Freezone may well constitute an important promotional tool for the respondent in differentiating its offerings to those of its competitors.

187 It is submitted by the respondent that the provision of Freezone has the effect of promoting the consumption of legitimate media, which itself has the effect of reducing the amount of copyright infringement occurring. Mr Phillipson, Mr Kaplan and Mr Perry (three

of the studio witnesses) gave evidence to the effect that it was their hope that the provision of legitimate means to gain access to copyright material online would reduce the consumption of copyright infringing material. Mr Gane gave similar evidence.

188 The Court accepts that the provision of Freezone would operate to promote the consumption of media, including media made available by the applicants, in a legitimate way, rather than consumption of that media in a copyright infringing manner. But whether Freezone actually reduces infringements as well as promoting non-infringing behaviour is another matter. Nevertheless, there is a likelihood that it must have had some such effect as the following exchanges with Mr Malone suggests:

> Well, that's a real attraction to somebody who is interested in illegal downloading, isn't it?---Or legal downloading.
>
> But certainly you would agree it's a huge attraction to a person interested in illegal downloading of films?---My understanding and belief is that accessing legal legitimate content substitutes for people that would otherwise be downloading illegal material.
>
> Would you agree-see if you can answer my question-you would agree Freezone is highly attractive to a person interested in maximising their bandwidth availability to engage in illegal downloading?---As I just clarified I don't believe that to be true.
>
> Why wouldn't it be true?---Because it's a different segment, it's a different type of person. People that are sitting there watching iView are not simultaneously watching a different movie.
>
> But they get Freezone anyway under your deal, don't they?---Yes. But this is a choice of what am I going to watch right now.
>
> …
>
> And they've got all the download they'd otherwise paid for, to illegally download, haven't they?---But they have a finite number of hours in their day, so by watching an ABC episode of Dr Who, they are now watching something that is legal, legitimate and provided for them by iiNet on attractive terms. That's an alternative to downloading something illegal.

The Court concludes that it is impossible to determine on the available evidence whether Freezone has in fact reduced the amount of infringements occurring and, if so, the extent of any reduction. Nevertheless, the Court finds that it is likely that it would have had some such effect to that end.

189 As the above exchanges also suggest, the applicants sought to argue that Freezone actually had the effect of promoting copyright infringement. An inference arises from the

above exchanges that the only non-infringing material available for download is that on the Freezone, the corollary being that downloads other than by way of Freezone must be of copyright infringing material.

190 The difficulty with the applicants' submissions is that, as will be discussed below at [239]-[250], the Court does not accept that bandwidth or quota usage can be equated to infringing activity. That is, making available quota as a result of using Freezone does not necessarily promote copyright infringement. The applicants' submission that Freezone promotes copyright infringement is predicated upon the basis that the only legitimate media that one could consume would be through the Freezone. This is simply not the case, as discussed at [245] below. Further, Mr Malone provided evidence in cross-examination that neither AFACT nor any copyright owner ever suggested that Freezone led to copyright infringement, or asked the respondent to shut down Freezone for that reason.

191 For these reasons, the Court rejects the arguments of the applicants that Freezone assists copyright infringement.

'Robot' notices

192 As well as the AFACT Notices, the respondent has received for many years emails alleging copyright infringement from the United States. Mr Malone has provided evidence that each day the respondent receives up to 350 of such emails. The Court has no evidence before it how these emails are generated, nor of any investigative process underlying the generation of such notices. Consequently, the Court does not find that such emails are reliable evidence of copyright infringement.

Respondent's witness – Stephen Joseph Dalby

193 Mr Dalby is the Chief Regulatory Officer of the respondent, a position which he has held since 2006. His duties have included the provision of guidance to the various iiNet business departments regarding regulatory issues. Mr Dalby has given a substantial amount of evidence which will be referred to where relevant. For present purposes the primary import of his evidence is of the respondent's treatment of the AFACT Notices.

194 The evidence establishes that, within the respondent's operations, Mr Dalby, rather than Mr Malone, was responsible for dealing with the AFACT Notices. In acting in response to those Notices Mr Dalby worked with Mr Parkinson who was the respondent's 'Credit Manager' and he reported to Mr Dalby on the matter. The applicants seek to challenge the respondent's failure to call Mr Parkinson. Such issue is dealt with at [216] and following. The Court will consider Mr Dalby's treatment of the AFACT Notices with the submissions relating to the credit of Mr Dalby, since the submissions on each issue are inextricably linked.

Credit of Mr Dalby

195 The applicants submitted, as with Mr Malone, that Mr Dalby was an unreliable witness, and that his evidence should not be relied upon except where it contradicted his interests or was otherwise corroborated.

196 There are three distinct issues which are submitted to undermine the credit of Mr Dalby as a witness. The first concerns alleged material factual oversights in the preparation of his affidavit regarding his treatment of the AFACT Notices; the second relates to his professed difficulty understanding certain aspects of those Notices; and the third regards his reference to (or rather lack thereof) the Telco Act defence.

PREPARATION OF AFFIDAVIT

197 The applicants submit that Mr Dalby provided an affidavit which, for two reasons, was likely to give a misleading impression to the Court concerning the receipt by the respondent of the AFACT Notices. Firstly, it is claimed that Mr Dalby never gave the impression in his affidavit that he had no intention of complying with the AFACT Notices irrespective of the amount of information AFACT provided in those Notices; and secondly that he gave the false impression in his affidavit that he and Mr Parkinson had determined the respondent's response to the AFACT Notices themselves, without mentioning that there were communications between Mr Dalby and Mr Parkinson and other ISPs that were part of the 'diss_connect' group.

198 The diss_connect group was an email list set up by the Internet Industry Association ('IIA'), the industry group for the internet industry. The Court rejected an application for such group to intervene in these proceedings on 26 November 2009: see *Roadshow Films Pty*

Ltd v iiNet Limited (No. 2) [2009] FCA 1391. The email list was set up for interested ISPs to share information regarding interactions with rights holders and copyright issues. Major ISPs represented in the list included the respondent, Telstra, Optus, Internode and AAPT.

199 As to the first issue, the Court rejects the applicants' characterisation of Mr Dalby's affidavit as misleading. He specifically said in such affidavit at [88]:

> As a result of the issues referred to above, namely:
>
> (a) the problems with the identification of iiNet account holders;
>
> (b) not understanding all of the information in the AFACT Letter; and
>
> (c) the nature of the demands made by AFACT,
>
> I decided that iiNet was not in a position to take any direct action against its subscribers based on the information contained in the AFACT Letter. To me, it was a straightforward decision as to my mind there were a lot of issues that made compliance with AFACT's demands unreasonable or impossible.

There was further evidence in his affidavit of his attitude on this issue at [91], but that portion of the affidavit was objected to on hearsay grounds and on this basis was rejected by the Court. Further, in the last email referred to by Mr Dalby in his affidavit that was sent to AFACT in regards to their notices on 12 August 2008, Mr Parkinson wrote:

> …iiNet will not take the responsibility of judge and jury in order to impose arbitrary and disproportionate penalties purely on the allegations of AFACT…
>
> AFACTs irrelevant assumption that iiNet has "no shortage of technically qualified employees…" is simply pointless. iiNet is not a law enforcement agency and has no obligation to employ skilled staff in pursuit of information for AFACT. AFACT is in no position to make such comment and it achieves nothing. If AFACT is not willing to invest its own resources to protecting [sic] its rights using the correct channels available IiNet [sic] is not going to.

The latter paragraph was written in reply to AFACT's answer to the respondent's first response to the first AFACT Notice. In the first response, the respondent's letter stated that Mr Parkinson did not understand some aspects of the AFACT Notices. Consequently, it was clear by the respondent's second response to AFACT that the respondent would not comply with AFACT's demands, irrespective of the level of detail included, or what explanation was provided. The Court finds that by including such evidence in his exhibit Mr Dalby made his position clear. The Court rejects the submission that Mr Dalby's credit is undermined because he did not spell out such point with exact words in the text of his affidavit. There was text to

that end in the affidavit and the exhibited emails made the respondent's, and Mr Dalby's, position quite clear.

200 As to the second issue, the applicants are correct in stating that Mr Dalby's affidavit does not describe the complete history of communications made between either himself or Mr Parkinson and the diss_connect group. However, this does not lead the Court to a finding that Mr Dalby's credit is adversely affected.

201 It was clear from Mr Dalby's affidavit that discussions were held between Mr Parkinson and Mr Dalby and other members of the diss_connect group at the time of drafting the respondent's response to the AFACT Notices. As mentioned, Telstra was a member of the diss_connect group and Ms Perrier was the Telstra representative. She distributed to the group a proposed draft 'straw man' response to the AFACT Notices. Such email and letter were exhibited to Mr Dalby's affidavit. This was evidence of collaboration between the members of the diss_connect group. Mr Dalby specifically explained at [34]-[43] of his affidavit (though some parts were rejected following objections) the broader context of the diss_connect group discussions in dealing with AFACT in 2008. In light of this, it was not necessary for Mr Dalby to mention each and every communication between himself and Mr Parkinson and the diss_connect group. The Court does not accept that Mr Dalby sought to mislead the Court in the preparation of his affidavit on the key issue of the respondent's response to the AFACT Notices.

202 As a separate ground to attack Mr Dalby's credit, the applicants relied upon Mr Dalby's answers to questions relating to a 'blog' published by the CEO of a competitor ISP. The evidence established that Mr John Linton of Exetel had published a blog which was hyperlinked to an email sent by Mr Parkinson to the diss_connect group on 9 July 2008. Such blog described Exetel's response to the AFACT Notices it was receiving. Mr Dalby repeatedly denied, in response to at least eight different questions, having read such blog. In explanation, Mr Dalby provided the following evidence regarding Mr Linton, '*I don't agree with his opinions and therefore was very unlikely then and now, to read his blog*' and '*I don't get my education on these sorts of matters from Exetel and wouldn't ever seek to do so*'. There is evidently antipathy between Exetel and the respondent, but such issue is irrelevant to

the current proceedings. As to the specific factual issue of whether Mr Dalby read Mr Linton's blog, based on such evidence the Court is not satisfied that Mr Dalby did so.

LACK OF UNDERSTANDING OF AFACT NOTICES

203 The applicants submit that Mr Dalby was misleading the Court when he suggested that he did not understand aspects of the DtecNet Notices and that for this reason there was not compliance by the respondent with such Notice's demands. Before engaging with such issue it is important to set out the factual history, although this may involve some repetition of facts referred to previously.

204 The first AFACT Notice was sent to the respondent on 2 July 2008. The second was sent the next week on 9 July 2008. The third was sent on 16 July 2008. The first two letters were sent with a CD accompanying the letter which contained the spreadsheet attached to the letter in electronic form. From the third letter onwards the letters were accompanied with a DVD containing the electronic version of the spreadsheet as well as the underlying data gathered by DtecNet discussed above at [113].

205 The first email sent in response to the AFACT notice of 2 July 2008 was sent by the respondent on 25 July 2008. In this email Mr Parkinson made clear that certain words contained in the spreadsheets were not understood. Mr Dalby deposed in his affidavit that there were certain concepts related to the AFACT Notices and data attached which he did not understand at that time.

206 The Court accepts that it is entirely possible that Mr Dalby did not understand the technical language used in the spreadsheet, and that Mr Parkinson did not either. The Court accepts that Mr Dalby might have known broadly what the letters alleged, but that does not mean he understood the precise technical nature of what was alleged, the terminology used, nor the implications, specific to the BitTorrent protocol, especially in view of the vast quantity of data which accompanied each AFACT Notice.

207 Upon receipt of a reply on 29 July 2008 from Mr Gane and AFACT to the respondent's letter of 25 July 2008 suggesting that the respondent ought to be able to understand the AFACT Notices, a second letter was drafted by Mr Dalby and Mr Parkinson.

This letter sent by email on 12 August 2008 suggested that, as extracted above at [199], the respondent would not be acting on such Notices even if it did understand them. The sequence of first and second letter, and the different considerations underlying each was plainly set out in the affidavit and exhibit. That is, the second letter made clear that Mr Parkinson's (and thus Mr Dalby's) inability to understand the contents of the AFACT Notices was not the only reason why the respondent would not be complying with AFACT's demands. Consequently, it could not be said that Mr Dalby suggested that difficulty in comprehension was the only reason why AFACT's demands were ignored. The Court does not believe that the applicants' assertions reflect adversely on Mr Dalby's credit.

208 A distinct issue arises, that being whether Mr Dalby and Mr Parkinson appreciated, following receipt of the third notice, that the DVD which accompanied each AFACT Notice contained the underlying data gathered by the DtecNet Agent. The evidence on this issue is inconclusive. It was clear from Mr Dalby's affidavit and cross-examination that he knew that the CD accompanying the first letter only contained the spreadsheet in electronic form. It appears that it was brought to his attention that there was a DVD, rather than a CD, attached to the third letter, but it is not clear whether that letter was read in detail, and whether Mr Dalby and Mr Parkinson understood that the subsequent AFACT Notices contained information additional to that previously supplied. It appears that Mr Dalby had formed a view by that stage that even if the AFACT Notices did contain more information, it was not the respondent's task to interpret it, and this would explain his command to Mr Parkinson not to attempt to analyse the DVD attached to the letter.

209 The applicants rely upon a further matter which they claim goes to Mr Dalby's credit. Mr Gane of AFACT was cross-examined upon the adequacy of the information provided by the AFACT Notices. The applicants submit that Mr Dalby had made the decision not to comply with the AFACT Notices irrespective of the information supplied. The applicants submit therefore that the cross-examination of Mr Gane on this subject was wholly inconsistent with Mr Dalby's intention not to respond and this reflects adversely upon Mr Dalby's credit.

210 Whether it was fair for Mr Gane to be so cross-examined is irrelevant to Mr Dalby's credibility. The actions of counsel for the respondent in cross-examining an applicants'

witness on subject matter which was inconsistent with Mr Dalby's evidence cannot impact on Mr Dalby's credibility. The applicants' submission is, in any event, misconceived. Two distinct issues arise. The first is whether the AFACT Notices objectively provided sufficient information for someone reading them to understand them. The second was whether this was the reason Mr Dalby chose not to comply with the demands made in those letters. It is possible for both propositions to be answered in the negative. That is, the Notices did not provide sufficient explanation to interpret them and nevertheless this was not the reason the respondent eventually chose not to comply with them.

211 The Court is unable to conclude whether Mr Dalby ultimately acquired a proper understanding of the AFACT Notices. However, as events unfolded, this fact became irrelevant for the respondent as it made plain that it would be taking no action in response to AFACT's claims.

TELCO ACT ISSUE

212 The Court has considered the submissions of the applicants on the final issue regarding Mr Dalby's credit, that being whether his credit is weakened because he conceded that the Telco Act defence was not '*in [his] mind*' at the time of drafting the respondent's response to the AFACT Notices.

213 The Court does not understand how such issue reflects adversely against Mr Dalby's credit. Mr Dalby did not discuss the Telco Act defence in his affidavit. He did mention the Telco Act in his affidavit, but not in the context of the Telco Act defence. If Mr Dalby was dishonest, it could be expected that he would say the opposite, that is, that he did think that the Telco Act prohibited him from acting on AFACT's demands. However, he never made such assertion, which operates in favour of finding for his honesty, not against it.

214 The respondent has made clear that, on its submission, from the perspective of the law of authorisation, the Telco Act defence does not require it to have been in the minds of anyone in the respondent's employ at the time of dealing with the AFACT Notices. This issue is considered later in the judgment in Part E2.

215 The Court finds that Mr Dalby has provided consistent evidence and there is no untruthful or misleading evidence of the kind relied upon by the applicants. The Court makes similar findings to the credit of Mr Dalby as it did of Mr Malone. Mr Dalby's demeanour was of a person who believed absolutely in the truth of what he was saying. The Court rejects the attack on Mr Dalby's credit.

Submissions regarding the respondent's failure to call more witnesses

216 The applicants submit that the respondent's failure to call Mr Parkinson, as well as any technical staff of the respondent, such as Mr Bader or Mr Yerramsetti (a Development Manager of the respondent), has resulted in insufficient evidence or less reliable evidence being put before the Court than should have been the case.

217 As to Mr Parkinson, the Court can draw no inferences from his failure to be called. In *Apand Pty Limited v The Kettle Chip Company Pty Limited* (1994) 62 FCR 474 at 490 the Full Court stated:

> In our opinion the principle of *Jones v Dunkel* would not be of assistance in these circumstances where, although the opinions and conduct of lesser officers of the appellant contributed to the decision-making process carried out by Mr Ballard and Mr Reeves on behalf of the corporation, the latter gave evidence of the decision they made and their reasons for doing so.

The respondent called Mr Dalby who was Mr Parkinson's superior. Although the letters to AFACT on behalf of the respondent were signed by Mr Parkinson, it was clear that Mr Dalby had oversight and responsibility for responding to AFACT. The Court draws no inference regarding Mr Parkinson not being called.

218 Similarly, the Court draws no inference regarding the failure of persons being called regarding the Westnet policy. As already explained above at [151]-[154], the Court does not believe that the Westnet policy was relevant for the current proceedings since Westnet never received any AFACT Notices, nor did it have any intention of acting on notices of infringement beyond passing them on to its subscribers. Both matters are crucial for the current proceedings.

219 The Court draws no inference from the respondent not calling its expert witness on technical matters, Dr Caloyannides. Much of his evidence was relevant to the claim

(abandoned by the applicants before the hearing commenced: see [14] above) which alleged that the respondent directly infringed copyright by making copies of the applicants' films. Much of the remainder of his evidence was relevant to issues which were adequately covered by Mr Carson and Mr Lokkegaard.

220 The Court draws no adverse inferences because the respondent did not call any technical staff. The Court considers that Mr Malone's technical background, as well as his ability to consult technical staff in the production of his affidavit, was sufficient to provide evidence of technical issues.

Respondent's witness – David Buckingham

221 Mr Buckingham is the Chief Financial Officer of the respondent and as such he is a member of the executive committee of the respondent and reports directly to Mr Malone. As Chief Financial Officer he has the responsibility for the respondent's financial performance, including management and reporting.

222 Mr Buckingham is responsible for the preparation of the respondent's external financial reports including a half-year financial report and annual report as well as monthly reporting. A significant amount of confidential financial information has been exhibited to Mr Buckingham's affidavit.

223 Mr Buckingham's primary evidence before the Court relates to the financial aspects of the respondent's business. Mr Buckingham was not cross-examined by the applicants. However, the applicants have challenged certain aspects of his evidence in their closing submissions and such matters are dealt with hereunder.

The respondent's financial interests – 'The iiNet business model'

224 One key issue in these proceedings was whether, as repeatedly submitted by the applicants, it was in the respondent's financial interests to have the iiNet users infringing and using ever larger amounts of their quota.

225 It is instructive to extract Mr Buckingham's affidavit evidence on this point:

> The profitability to iiNet of each individual customer is contributed to by the extent

> of that customer's usage of bandwidth in relation to the plan to which that customer subscribes…
>
> …I consider that the examples (and the financial data upon which they are based) demonstrate that the most profitable customer for iiNet is the customer who signs up for a large quota (and pays the higher subscription fee for the large quota) but does not use it.
>
> The examples shown above also indicate the high volatility, in terms of financial performance for iiNet, of customers who subscribe to high quota plans. It is beyond the control of iiNet how much of their quota customers use. On the high quota plans, the extent of the customers' usage of the available high quota makes a very significant difference to EBITDA to iiNet in respect of that customer. The ideal customer from iiNet's perspective is a customer who enrols in Home 2, Home 3, Home 4 or Home 5 plan (which do not have the financial volatility of the very high quota plans) and who does not use more than the average amount of the quota available to them…Home 6 and Home 7 plan customers are not the ideal customers, despite the high subscriber fees paid by them, by reason of the potential significantly higher costs if they use the full amount of their quota.

226 The applicants submit that the confidential evidence of Mr Buckingham demonstrates that gross margins and EBITDA (earnings before interest, tax, depreciation and amortisation) are higher for higher plans, that is, the respondent derives more revenue from higher plans.

227 Such submission is correct, but it overlooks two factors. The first is that such submission does not alter the fact that volatility of revenue per subscriber may well be an important business consideration for the respondent. It is instructive to compare two 'Home' plans. While such plans are not the only plans available from the respondent, the Court considers them to be a useful sample. Although the underlying data is confidential it is necessary to refer to it in order to demonstrate the point.

228 An unbundled (that is, provision of the internet only) Home 3 plan and an unbundled Home 7 plan (the plan Mr Herps signed up to) will be compared. Under the Home 3 plan, fixed costs (for example, port allocation, support costs and variable on-costs which are largely fixed per account) account for 39.9% of revenue. Variable costs (bandwidth, calculated by multiplying the raw cost per gigabyte by the number of gigabytes allocated by each plan) are a mere 5.7% of revenue. Therefore, the costs of the plan are highly predictable and stable. Under the Home 7 plan, fixed costs account for 16.6% of revenue and variable costs account for 55% of revenue. This disparity may result in a situation in which costs on an account by account basis are highly variable and unpredictable. A subscriber may use very little quota, equally they may use a vast amount, significantly reducing profitability.

229 The evidence clearly indicates that the relatively more profitable accounts, on an account by account basis, are the lower bandwidth accounts. Potential profit over revenue (an approximate measure of profitability) could vary between 83.5% to 28.4% under the Home 7 plan (the difference between using all or none of the bandwidth allocated), but the range would only be 60.1% to 54.4% in relation to the Home 3 plan. Therefore, while it is possible for a Home 7 plan to be relatively more profitable (if no bandwidth is used) than Home 3, it is far more certain that the Home 3 plan will be more profitable. Certainty of profitability and therefore income is obviously a highly important consideration for a business. The Home 7 plan may produce more absolute revenue to the respondent even if it is not more profitable, but that is not the only relevant consideration.

230 The applicants simultaneously submitted that one need not consider Mr Buckingham's evidence on the issue given the evidence of Mr Malone. The applicants submit that Mr Malone's evidence indicates that there is a simple financial interest for the respondent in the iiNet users infringing and consuming ever larger quantities of bandwidth. However, the Court finds that, at best, Mr Malone conceded that revenue was greater the higher the plan, but as much has been demonstrated above. Mr Malone stressed the distinction between profit and revenue:

> But by the same token, you are not in a position to earn more revenue by offering higher quotas unless you actually acquire more bandwidth yourself?---Revenue and profit are not the same in this context. Yes.
>
> But the ideal outcome for the business, is it not, is to push people on to the highest plans, to pay more, **but not use all the bandwidth that they offer**?---From a profitability point of view, yes, that is correct.
>
> …
>
> And it's in your interests, isn't it, to sell more and more higher quotas; isn't it?---No.
>
> That's where your revenue comes from?---Yes.
>
> It's in your interests to sell higher quotas because you get more money, don't you?---**But not more profit**.
>
> Whether you get more profit depends on how much of the quota is used, isn't it?---Yes.
>
> But in a perfect world, maximising sale of quota **which is not used**, leads to maximum profit; correct?---Yes.

231 These extracts and portions in bold demonstrate that Mr Malone was at pains to emphasise the same point as Mr Buckingham, namely that profitability depends on the

bandwidth used by iiNet users. Even if Mr Malone's evidence suggests to the contrary and contradicts the evidence of Mr Buckingham, the Court prefers the evidence of Mr Buckingham, given that he produced evidence of the actual financial data of the respondent.

232 Ignoring the aspect of profitability and looking at raw revenue, the Court accepts that higher plans generate more revenue. However, it is important to bear in mind the applicants' contention. They argue that it is in the respondent's interests to have its subscribers using ever increasing amounts of bandwidth, increased bandwidth being assumed to lead to increased infringement (erroneously, as discussed below at [239]-[250]). The answer, on the evidence, is that it is in the respondent's interests to have iiNet users consuming ever increasing amounts of bandwidth, but with an important qualification.

233 It is clearly in the respondent's interests to have its subscribers using greater amounts of bandwidth, but only if that greater amount of bandwidth usage correlates with larger numbers of subscribers moving up to more expensive plans. If subscribers use ever increasing amounts of bandwidth but remain on their existing plan and do not upgrade their plan, this would operate against the respondent's financial interests. It simply cannot be assumed that subscribers will upgrade to higher plans even if they regularly reach their quota, given that, of the Home plans (unbundled and otherwise) 1% of the respondent's residential subscribers are on Home 7, 3% on Home 6, 17% on Home 5, 14% on Home 4, 30% on Home 3, 29% on Home 2 and 4% on Home 1 (the numbers are rounded and accordingly do not reconcile exactly to 100%). That is, there are barely more subscribers on Home 4-7 plans combined than there is on the low quota Home 2 or 3 plans individually.

234 This evidence does not suggest that a substantial number of subscribers are being persuaded to take up more expensive and higher quota plans. It certainly does not suggest that the respondent is yielding a substantial proportion of its revenue from subscribers on high quota plans.

235 Further, of the RC-20 accounts, only half of the subscribers moved up to a higher plan in the period examined, and one of those ten subsequently downgraded back to their original plan. That is, less than half of the group that would be expected to be the prime group to demonstrate that it was in the respondent's interests for people to infringe, acted in the respondent's interests by upgrading their plans. In contrast, of those 20 subscribers, 15 used

up their full monthly quota regularly, suggesting that they were not ideal subscribers from the respondent's perspective given that they used all their quota, making them the least profitable subscribers within their particular plan. This example of 75% of the group regularly reaching 100% of the monthly quota can be compared with the average monthly usage of quota of 38% across all accounts on Home plans. In summary, at least compared to the small sample group of infringers the Court has before it, infringers do not seem to be the ideal subscribers from the respondent's financial perspective.

236 The applicants also point to the fact that the respondent makes it easier to upgrade plans, rather than downgrading plans (by charging to downgrade but not upgrade), as well as its suggestion to subscribers via email to consider upgrading their plan when they reach their quota, as evidence of it being in the respondent's commercial interest for the iiNet users to infringe and consume more bandwidth.

237 The Court does not consider that such claim is established. It may be assumed, as already found, that it is in the respondent's interests for subscribers to use more bandwidth if it leads to them upgrading their plans. But, as the evidence demonstrates, this does not necessarily occur. Further, it would be in the respondent's interests for subscribers to move to high plans whether infringements were occurring or not occurring. From a financial perspective, the respondent is indifferent as to the use made of bandwidth. If, as the evidence suggests, those that do infringe do not always upgrade, but usually do consume all their quota each month, then such users are again not, from a financial perspective, the preferred subscriber for the respondent.

238 In conclusion, the applicants have not made out their proposition that it is in the interests of the respondent either to have the iiNet users using ever increasing amounts of bandwidth, or that it is in the respondent's interests to have the iiNet users infringing.

Is 'bandwidth', 'downloading' or 'quota use' necessarily infringing?

239 One of the more adventurous submissions the applicants appeared to make in these proceedings was that bandwidth, downloading or quota usage by iiNet users could be considered synonymous with copyright infringing behaviour.

240 To so conclude, two propositions would have to be accepted. First, the Court would have to accept that the vast majority of BitTorrent usage infringes the applicants' copyright. Secondly, the Court would have to accept that the vast majority of the bandwidth used by the respondent's subscribers was related to BitTorrent usage. Such propositions might have had weight in relation to the Kazaa system and Mr Cooper's website in *Kazaa* and *Cooper* 150 FCR 1 (as discussed further below at [362] and [363] respectively), but they do not apply in the present circumstances.

241 As to the first and second proposition, the acceptance of Mr Malone of the following suggestion, put at various times in the proceedings, should be noted:

> At the time of first receipt of the AFACT notices, you understood, that is in the middle of 2008, as you have agreed, or assessed, that more than half by volume at least, traffic over your service was represented by BitTorrent downloads or uploads?--Yes.

Mr Malone also accepted that a significant proportion of such downloading or uploading would comprise material which infringes copyright. The Court accepts that this is a possibility, but is not persuaded merely by the evidence of Mr Malone that this is established, simply because there is no possibility factually that either Mr Malone or anyone else could conclusively know that. The Ipoque reports on internet traffic tendered by Mr Gane regard BitTorrent traffic flowing across the internet in general, not the makeup of that traffic specifically. There is simply no evidence before this Court of the extent of BitTorrent traffic which involves infringing material and, more importantly, what proportion of that traffic involves material infringing the copyright *of the applicants*.

242 There is evidence before the Court of examples of the use of BitTorrent that is legitimate, that is, use that does not infringe anyone's copyright. One example is the distribution of media, for example games such as World of Warcraft (a highly popular game with many millions of players) and television programs, such as Joost. The operating system Linux (an open-source competitor to Microsoft Windows) is also distributed by means of BitTorrent. While these examples are unlikely to account for a large proportion of BitTorrent traffic, they will constitute some proportion of that traffic.

243 Secondly, even if the Court was to assume (for the purposes of this analysis only) that the predominant use of the BitTorrent system is to infringe copyright, as was found of the

Kazaa system and Mr Cooper's website, there is no evidence of the proportion of traffic which involves the infringement of the applicants' films. There is much other infringing media that could be shared via the BitTorrent system. For example, exhibit RR, which was a print out of a section of The Pirate Bay website (submitted to be a major source of .torrent files relating to infringing content) includes, as part of its search function, the ability to search only specific types of media, such as '*Audio*', '*Video*', '*Applications*', '*Games*' and '*Other*'. Only one of these media types represents the copyright material of the applicants. Even within '*Video*', there are many kinds of videos which could be searched that would not be owned by the applicants, such as pornographic videos. A quick glance over the '*Search Cloud*' (which would appear to be the frequently searched terms on The Pirate Bay) suggests that while some of the search terms relate to the applicants' material, most do not. Most appear to relate to games, computer applications, pornographic material and audio, none of which constitutes subject matter owned by the applicants.

244 Therefore, even making the assumption that *all* BitTorrent traffic relates to infringing material (again, for the purpose of this analysis), the Court can make no findings that the majority of that traffic necessarily relates to the applicants' films and television programs. The proceedings before the Court relate to the infringement of the applicants' copyright, not the infringement of copyright in the abstract: see *WEA International Inc and Another v Hanimex Corporation Ltd* (1987) 17 FCR 274 ('*Hanimex*') at 288. The respondent must authorise the infringement of the *applicants'* copyright for their claim against the respondent to succeed. While there can be no doubt that infringements of the applicants' copyright are occurring by means of the BitTorrent system, there is insufficient evidence before the Court to determine whether infringement of the applicants' copyright is the major, or even a substantial, part of the total BitTorrent traffic. This should be contrasted with *Kazaa* and *Cooper* 150 FCR 1 when the applicants in those proceedings were *music* companies and, as a matter of fact, it was known that Mr Cooper's website was being used almost exclusively for infringing *music* files (after all, it was called www.mp3s4free.net) and the Kazaa system appeared to be used for, or was considered by its users to be, '*a free music downloading search engine*': see *Kazaa* at [151]. That is, the means by which the infringements occurred in those proceedings were clearly being predominantly used to infringe the applicants' copyright in those proceedings. The evidence is not the same in these proceedings.

245 There is ample evidence before this Court of material which uses significant amounts of bandwidth or quota which is not infringing. Further, there is evidence that most of that material is outside the Freezone. For example, there is evidence that Channels 10, 9, 7 and SBS all allow streaming of television programs or parts of television programs from their websites. As mentioned, the ABC does so also but its content is within the Freezone. Foxtel, TiVo and Telstra Bigpond allow film and television program downloads/streaming. These are, of course, not the only examples. There are too many to list. But they do provide evidence which destroys the applicants' characterisation of bandwidth, quota usage or downloading as necessarily or frequently constituting copyright infringing activity.

246 The Court notes the following increasingly exasperated responses by Mr Malone on this issue in his cross-examination:

> But you have no policy which suggests to customer service representatives that they should discourage any use of BitTorrent client; that's correct?---Yes.
>
> And or even discouraging any downloads using BitTorrent; there's no policy in relation to that, is there?---Downloading by BitTorrent is not in itself an offence.
>
> …
>
> But still have all the bandwidth they paid for available for downloading?---Yes.
>
> Well, that's a real attraction to somebody who is interested in illegal downloading, isn't it?---Or legal downloading.
>
> …
>
> But you promote as a benefit of Freezone as freeing up customer's quota for, amongst other things, downloading, don't you?---Yes, but not all downloading is downloading of illegitimate material or movies, there's plenty of other things to download on the internet.
>
> …
>
> Unauthorised downloaders are the sort of customers who need more and more bandwidth; you agree?---No. I think again you're trying to paint all downloads as illegal.

Mr Malone said in re-examination:

> And when one uses the internet, what is-what are the things one could be doing when one is downloading?---Receiving an email, browsing the website, on-line gaming, watching television, listening to the radio, downloading a file, the list-VPNs to businesses, downloading files from work, the list is endless.

247 The Court has specific examples of subscriber accounts which are alleged to have infringed the applicants' copyright in the RC-20 accounts. Schedule 1 of the respondent's closing submissions demonstrates that, on the evidence before the Court, it is impossible to conclude that even a substantial amount of monthly quota of those subscribers was being used to infringe the applicants' copyright.

248 The applicants submit that Schedule 1 is unreliable because three of the RC-20 accounts were Naked DSL plans. Uploads as well as downloads count toward quota on Naked DSL plans. While it is possible on the evidence to know how much each RC-20 account subscriber has downloaded in respect of each film, it is impossible to know the extent of the uploading. Consequently, it is submitted that the Naked DSL subscribers might have used much of their quota uploading, which would not be displayed in Schedule 1.

249 The Court accepts this submission. However, even ignoring those three accounts, the point is still made by Schedule 1 that on the evidence before the Court in relation to the RC-20 accounts generally, in most cases less than 10% of monthly quota was being used to infringe the applicants' copyright. Even assuming that the applicants are correct in their submission that this does not represent the total amount of infringement of the applicants' copyright being carried out by these iiNet users, the total amount of infringement of their copyright would have to be substantially greater than what has been led in evidence in relation to these users to demonstrate that even a majority of that quota was used for the purpose of infringing the applicants' copyright.

250 The above analysis is not intended to be dismissive of the infringer's conduct. However, it demonstrates that the claim made throughout these proceedings that bandwidth usage or downloading is somehow necessarily, predominantly or even significantly copyright infringing, is simply not established on the evidence. The Court finds the applicants' attempt to cast a pall over internet usage, such that it is assumed to be infringing, unless otherwise shown, is unjustified. The Court does not find that there is any evidence that the majority or even a substantial usage of the bandwidth allocated by the respondent to its subscribers relates to the infringement of the applicants' copyright.

Proof of infringement – catalogue vs identified films

251 Following from the judgment in this matter in *Roadshow Films Pty Ltd and Others (ACN 100 746 870) v iiNet Limited (ACN 068 628 937)* (2009) 81 IPR 99 (‘*Roadshow No. 1*’) the Court divided these proceedings into a determination of liability (this judgment) and quantum of relief. Also in that decision the Court rejected at [52]-[54] a motion of the respondent to confine this hearing only to the 86 identified films for which copyright ownership and subsistence was specifically pleaded.

252 In making such decision the Court was concerned to ensure that, should liability be established, the applicants would be able to seek relief in relation to the entire catalogue of their films after proving infringement in relation to the more specific 86 identified films. However, this procedure gave rise to an unanticipated complication in these proceedings in that the applicants provided evidence before the Court of alleged infringements involving both catalogue and identified films. Nevertheless the Court does not consider that the issue is of any real importance. As will be made clear by Part D of this decision, there is sufficient evidence of infringement to make a finding that iiNet users have infringed the applicants’ copyright irrespective of whether evidence of infringements relating to catalogue films is considered.

PART D: PRIMARY INFRINGEMENT

253 The Court accepts that copyright subsists in, and the applicants own (or are the exclusive licensees of) the copyright in the 86 identified films. The Court accepts that these films are cinematograph films as defined in s 10 of the Copyright Act.

254 The Court accepts that, pursuant to ss 115(1) and 119(a) of the Copyright Act, the applicants, as owners and exclusive licensees of the 86 identified films, have the right to bring this action for copyright infringement.

255 Section 101 of the Copyright Act states that:

> (1) Subject to this Act, a copyright subsisting by virtue of this Part is infringed by a person [the respondent] who, not being the owner of the copyright, and without the licence of the owner of the copyright, does in Australia, or authorizes the doing in Australia of, any act comprised in the copyright.

256 As a prelude to any finding of authorisation by the respondent, a finding must be made that copyright infringing acts were committed by persons that were authorised by the respondent. As much was made clear by Gummow J in *Hanimex* at 287-288 where his Honour found that one does not authorise actions in the abstract. Rather, one must authorise particular acts which have to be proven before a Court. This is what is known as 'primary' infringement.

257 In general, the respondent has conceded that there have been primary infringements committed by iiNet users. However, it argues that the Court must undertake a close analysis of the character and scope of those infringements. In order to do so, a detailed analysis of the statutory provisions in the Copyright Act is necessary.

The authorisation of acts, not of persons

258 As a brief aside, one issue should be referred to at this point. The applicants place significant weight in the fact that authorisation must be authorisation of *acts*, not of *people*. They cite the wording of s 101 of the Copyright Act, particularly the following part: '*…authorizes the doing in Australia of...any* ***act*** *comprised in the copyright*' [emphasis added].

259 Based upon such text, the applicants argue that there is no need for them to prove the exact identities of any person who is directly infringing. Consequently, they claim that it is not necessary for them to prove that the respondent authorised a particular person or persons to carry out an act that is copyright and rely upon *Kazaa* and *Cooper* 150 FCR 1 which proceeded upon the basis that the identities of the primary infringers were unknown. However, the applicants' interpretation of the statute, namely that they need only prove that the respondent authorised particular *acts*, can be misleading.

260 While one may authorise an act, those acts are done by people: that is, there can be no doubt that there must be primary infringement by a legal *person* or *persons*. A computer cannot infringe copyright. A computer can aid in the infringement of copyright; indeed a computer is essential in order to infringe much copyright, such as the right to 'electronically transmit to the public or 'make available online' to the public. However, this must not distract

from, and the focus on acts authorised must not lose sight of, the fact that the respondent, to breach copyright, must authorise infringing acts done by a person or persons.

261 For example, the cinematograph film copyrights referred to in the Copyright Act are the right to copy the film s 86(a), to communicate the film to the public s 86(c) and to cause the film to be seen and/or heard in public s 86(b). All such acts *must* be done by legal persons, even if, strictly speaking, they are brought about by technical means. Further support for such proposition is seen in s 101(1A)(b) of the Copyright Act which states: '*the nature of any relationship existing between the person [the respondent] and* ***the person who did the act concerned***' [emphasis added]. See also the decision of Gummow J in *Hanimex* at 287 in which his Honour found '*it has not even been shown that there has been any* ***unauthorised reproduction by any particular person*** *of any of the sound recordings in which the applicants hold copyright*' [emphasis added]. Such finding suggests that his Honour believed that the relevant primary infringement must be committed by a person.

262 Further, the applicants' construction of the Copyright Act ignores the finding of Wilcox J in *Kazaa* at [358] where his Honour said '*[t]he authorisation referred to in s 101(1) extends only to direct authorisation, by a potential defendant, of the person who performs the infringing acts*' and at [415], '*[t]here is no evidence as to the identity of the particular Kazaa user or users who made available for sharing, or downloaded from another user, each of the defined recordings. However,* ***somebody*** *must have done so*' [emphasis added]. These statements suggest that a party such as the respondent must authorise persons, not acts.

263 Therefore, while s 101 states that the respondent must authorise acts, and not people, this proposition is of no consequence when it is understood that those acts must be done by persons. Whether or not the respondent must authorise acts is accordingly not germane. As will become apparent, such perspective is an important one to keep in mind when considering whether or not activities constitute primary infringement.

Nature of the primary infringements

264 There has been extensive argument in these proceedings regarding the nature of the primary infringements which have occurred. This is notable, as it appears that argument was not so extensive before their Honours Wilcox J and Tamberlin J in the *Kazaa* and *Cooper* 150

FCR 1 proceedings respectively, given the brief manner in which their Honours addressed the issue in their decisions. Indeed, their Honours' judgments treat the proof of primary infringement as virtually an assumed conclusion. Such approach may be appropriate in some circumstances, but not in all. Since authorisation is predicated upon copyright infringing acts occurring, the nature and extent of those acts must be ascertained.

265 The respondent virtually conceded that proof of primary infringements would be made out by the applicants but argued that it is essential that the Court identify those primary infringements in respect of which the applicants have led evidence. The Court agrees. A finding of the character of the primary infringements committed by the iiNet users is necessary for two reasons. The first reason is to establish whether the respondent authorised those specific acts and persons. The second reason is because the nature and extent of the primary infringements will be relevant to the scope of the relief available to the applicants, should the respondent be found to be liable for those primary infringements because it authorised them.

266 As mentioned, s 101 of the Copyright Act states that one will infringe copyright where one does an act that is copyright in relation to a subject matter without the licence of the copyright owner or exclusive licensee. The relevant copyright acts in relation to the applicants' cinematograph films are found in s 86 of the Copyright Act. Such section relevantly states:

> For the purposes of this Act, unless the contrary intention appears, copyright, in relation to a cinematograph film, is the exclusive right to do all or any of the following acts:
>
> (a) to make a copy of the film;
>
> (b) …
>
> (c) to communicate the film to the public.

Section 86(c) is often referred to as the 'communication right'. It was adopted into the Copyright Act pursuant to the *Copyright Amendment (Digital Agenda) Act 2000* (Cth) ('*Copyright Amendment (Digital Agenda) Act*').

267 The term 'communicate' is relevantly further defined in s 10 of the Copyright Act:

> ***communicate*** means make available online or electronically transmit (whether over a

> path, or a combination of paths, provided by a material substance or otherwise) … other subject matter…

268 A further provision of relevance is s 14 of the Copyright Act which relevantly states:

> (1) In this Act, unless the contrary intention appears:
>
> (a) a reference to the doing of an act in relation to…other subject-matter shall be read as including a reference to the doing of that act in relation to a substantial part of the…other subject matter…

269 Therefore, for the purposes of the present proceedings, there are relevantly three different exclusive rights of the applicants which may be infringed by iiNet users:

1. The right to make a copy of a substantial part of a film;
2. The right to 'make available online' a substantial part of a film to the public;
3. The right to 'electronically transmit' a substantial part of a film to the public.

The dispute

270 While the respondent concedes that infringements of copyright have been committed by iiNet users, a dispute exists between the parties of the number of those infringements and of the way in which they have been assessed. The respondent objects to the characterisation of the number of infringements alleged by the applicants, stating that, based upon the respondent's interpretation of the particular statutory provisions and method of assessment, these are grossly disproportionate to the reality.

271 The difference between the parties concerning the number of infringements results from their contrasting characterisations of the particular statutory provisions. Such contrasting characterisations are technical (both as to fact and as to law) but they are important, and were rightly the subject of extensive submission. Consequently, the Court will deal with each type of infringement in turn, to establish the correct characterisation of the provisions in relation to these proceedings.

'Make available online' a substantial part of the film to the public

272 Pursuant to the '*Statement of Nature of Case*' discussed at [22], the respondent admitted, for the purposes of these proceedings, that where the AFACT Notices show a

particular IP address at a particular time sharing 100% of a film, the person using the particular computer on which that file is stored and through which that file is connected to the internet (via the respondent's facilities), was making the film available online: that is, was committing an act of copyright infringement. The respondent, for the purposes of minimising the issues in dispute, also admitted in closing submissions that where the DtecNet evidence shows an iiNet user sharing less than 100% of the file, that user was nevertheless 'making that film available online'. The relevance of the percentage of film shared lies in the concept of 'substantial part' pursuant to s 14 of the Copyright Act which is extracted at [268] above.

273 The doctrine of 'substantial part' operates such that where someone does an act that is in the copyright of the applicants (copying, 'making available online' and so forth), but only does so in relation to a part of the work or other subject matter that does not constitute a substantial part, that act will not constitute an infringement of copyright. Or, to put it another way, the Copyright Act only grants the copyright owner the exclusive right to do the copyright acts in relation to a substantial part of the work or other subject matter.

274 The respondent argues that in the circumstance that the AFACT Notices show that a particular iiNet user is sharing less than 100% of the film, it would have to be established on a case by case basis whether the part being shared was, in fact, a substantial part. However, for the purposes of these proceedings, the respondent does not raise such issue. Regardless, the evidence establishes that the overwhelming majority of alleged 'making available online' infringements (78%) are in relation to 100% of the film being shared.

275 Therefore within these proceedings it is admitted by the respondent that the applicants' films have been 'made available online' by iiNet users. The dispute that remains is whether one makes a film available online once, or multiple times. In order to resolve that dispute, one must appreciate how an iiNet user's computer is connected to the internet, particularly in the context of the BitTorrent protocol.

Repeat infringers?

276 As explained at [113] above, the DtecNet Agent logs every incidence of downloading a piece of a file of a film from a particular IP address which is an IP address associated with the respondent. However, as the repeat infringer bundles produced as part of the evidence of

Mr Williams in MJW-1 and MJW-8 make clear, there may be multiple incidents of pieces being downloaded from what the evidence establishes is obviously the same computer.

277 The evidence of Mr Williams establishes by means of the PeerID that the same computer was the source of more than one alleged infringement. As discussed at [115] above, the PeerID is a random number generated by the BitTorrent client, upon the BitTorrent client being initiated. The PeerID exists until the BitTorrent client is closed. Upon reopening the BitTorrent client a new PeerID is generated. The PeerID is quite separate from an IP address, and it is important not to confuse the two.

278 Part of the PeerID identifies the particular BitTorrent client being used (for example, uTorrent), but the rest of the number is randomly generated. This number is broadcast to the swarm, that is, any peer in the swarm (such as the DtecNet Agent) is able to see the PeerID of any other peer in the swarm. Given that the number is generated by the BitTorrent client, and such client is a program on a particular computer, the inference arises that where one sees the same PeerID across multiple incidences of alleged infringement in the AFACT Notices, each of those alleged infringements was sourced from the same computer. This also means that even where the IP address changes, it can still be fairly assumed that the same computer is being used, albeit that the dynamic allocation of IP addresses by the respondent will lead to that computer being connected to the internet through a different IP address. While it is possible for two different BitTorrent clients on two different computers to generate the same PeerID, the length of the number and its random nature renders it highly unlikely that this will occur. Therefore, the Court accepts that where the DtecNet Agent downloads two or more pieces from the same PeerID, those pieces emanated from the same computer and were initiated by the same person.

How DtecNet produces multiple allegations of infringement

279 As already stated, the evidence in MJW-1 and MJW-8 demonstrates that on many occasions there are multiple incidents of a piece of the same file being downloaded by the DtecNet Agent from the same computer. There are two reasons why the DtecNet Agent might download more than one piece of the same file from the same computer.

280 Firstly, from the point of view of the DtecNet Agent as a peer in the swarm, each IP address represents a different computer. However, as the repeat infringer bundles and the above explanation demonstrates, this is not necessarily the case. The respondent assigns IP addresses dynamically, with the consequence that, over time, one subscriber account will be associated with multiple IP addresses, and therefore a computer accessing the internet through that subscriber account will have multiple IP addresses associated with it, although no more than one at any given time. The DtecNet Agent is calibrated to seek to download a piece of the file from every IP address which is associated with the respondent, even though, as the evidence indicates, these IP addresses will not necessarily correspond to different computers. This will mean that where an IP address by which a computer connects to the internet changes, the DtecNet Agent will download a piece of that file from that computer again, even though it is the same computer. This may generate a significant number of allegations of infringement in a short period of time. For example, the first page of MJW-8 discloses that the computer with the PeerID 2D5554313832302D7A38210B4FB71A1D53FE14B7 accessed the internet through at least 15 different IP address on 16 June 2009, in some cases with multiple different IP addresses within an hour. This was, on the evidence, by no means unusual.

281 Secondly, according to the evidence in relation to the 'peer suspension' feature of the DtecNet Agent from Mr Lokkegaard, the DtecNet Agent is calibrated to download a piece from the same IP address once every 24 hours. Therefore, in the circumstance where one subscriber account is associated with the one IP address (and therefore the one computer associated with the same IP address) over a period of more than 24 hours, it is possible for the DtecNet Agent to obtain more than one piece from that computer. For example, if the one computer accessed the internet through one IP address and participated in a swarm for three days, the DtecNet Agent would download three pieces from that IP address over three days.

282 The following issue arises from this technical analysis: the applicants assert that a separate 'making available online' infringement occurs every time one of their films is connected (or reconnected) to the internet, or, more precisely, to the BitTorrent swarm (the causes of which are referred to below). The respondent disagrees.

283 A connection or reconnection of copyright infringing material to the internet may occur for any number of reasons. The computer containing the file could be turned off, or

alternatively the BitTorrent client could be closed. This would disconnect that iiNet user/peer from the swarm, thereby making the file no longer available online (at least from that computer). When the computer is turned on and/or the BitTorrent client restarted, that file would again become available from that computer to the swarm. However, from the point of view of the DtecNet Agent, it would not necessarily be apparent that the file was not available for the time that the computer was turned off, or BitTorrent client closed. This follows from the fact that IP addresses are associated with a particular modem or router, and if the modem or router is never turned off (but a computer is) there is no way of knowing that that computer has become disconnected from the swarm other than from the lack of pieces downloaded by the DtecNet Agent in that period. Therefore, if an IP address allocated to a particular subscriber account did not change over a week, but the computer on which the file was stored was turned on and off (and with the BitTorrent client being opened and closed) multiple times over that period, that would not be known from the perspective of the DtecNet Agent. The AFACT Notices, based upon the DtecNet information, would accordingly not reflect the true position. In summary, there would be no way of knowing how often the file was disconnected and reconnected to the internet.

284 Further, the dynamic allocation of IP addresses may mean that a subscriber account is associated with multiple IP addresses over a short period of time, without a person connected to the internet through that account being at all aware of it. Each time the IP address changes, that computer is disconnected and reconnected to the internet. The evidence of Mr Carson and Mr Malone indicated that at most this process may cause an iiNet user to experience a momentary slowing of the speed of the internet. As stated, MJW-1 and MJW-8 demonstrated that in some circumstances the same subscriber account was disconnected and reconnected to the internet (with a new IP address) many times even within an hour. From the DtecNet Agent's perspective this represents multiple different computers sharing the file in the swarm, and each incidence will be logged as such, even if it is in fact the same computer. On the submissions of the applicants, that would be multiple cases of infringement by 'making available online'.

Correct construction of 'make available online'

285 The applicants claim that a new 'make available online' infringement occurs each time an iiNet user is disconnected and reconnected to the internet. Further, the applicants

submit that even if this not be the case, there must be a temporal aspect to the 'making available online' act such that infringements over a long period of time could constitute more than one infringement.

286 The appropriate response of the Court is to apply a reasonable construction of the term 'make available online'. Tamberlin J at [61] of *Cooper* 150 FCR 1 approved a construction of the term 'make available online' which favoured an approach that gave those words their ordinary meaning, and considered them in concert, rather than individually.

287 The Copyright Act, as mentioned, focuses on the actions of persons, not computers. *A person* makes a file available online and infringes copyright, not computers. Where copyright infringement is concerned, the technical process by which the connection to the internet is effected does not render one person a repeat infringer, and another a single infringer. Such an approach would suggest that those that have static IP addresses would infringe less than those that have dynamic IP addresses, because those with dynamic IP addresses will be disconnected and reconnected to the internet more frequently. It also necessarily follows from the applicants' reasoning (though no such submission has been made) that a person who turns off their computer every day will be a repeat infringer, while one who leaves it on will only infringe once.

288 Accordingly, the act of 'making available online' ought not to focus upon the technical process by which the file is 'made available online': rather it should focus on the substantive acts of persons. Leaving aside the exceptional (and highly unlikely) case of a person who deliberately seeks to acquire the same film repeatedly through the BitTorrent system (which does not arise from the facts before the Court), a person makes each film available online *once* through the BitTorrent system. The computer on which that file is stored, and from which pieces flow to the swarm, may be disconnected temporarily either because of the actions of the person, or because of the technical processes by which the respondent allocates IP addresses, but this does not have the consequence that such disconnection and reconnection ought to give rise to a new infringement of copyright on each occasion. The applicants' submissions render it virtually impossible for multiple infringements of 'making available online' not to occur. No doubt such interpretation would favour the applicants, but that does not necessarily mean it is the correct conclusion.

289 There is another factor which mitigates against the applicants' construction. The applicants' interpretation renders it virtually impossible to assess the number of repeat infringements occurring. As mentioned, there are multiple possible factors which could cause a film being shared by a peer in a swarm to be disconnected and then reconnected to the internet. First, the BitTorrent client could be closed down and reopened. Second, the computer could be turned off then turned on. Third, the router could be turned off and then turned on. Fourth, the modem could be turned off and then turned on. Fifth, the IP address which the subscriber account has been allocated by the respondent could change, necessitating a disconnection and reconnection to the internet. Sixth, there could be some issue at the ISP level or at the physical facility level (for example fallen telephone lines) which could cause a disconnection and eventual reconnection. Any one of these events, on the applicants' reasoning, would cause a new 'making available online' infringement. But the DtecNet evidence combined with the respondent's log in/log out details (such as with the RC-20 accounts) can do no more than confirm the fifth factor mentioned above. Some of the other factors could be proven with other evidence, but others, such as when and how often a computer is turned off, or a BitTorrent client opened and closed, are virtually impossible to prove.

290 The Court is of the opinion that these factors provide further reason to reject the applicants' interpretation of 'make available online' and to favour a construction that finds that each film is 'made available online' once, albeit perhaps for an extended period of time and, on occasion, not being accessible for periods of time, such as when the computer is turned off.

291 The applicants argue against the construction now found by the Court because it renders an incident where a film is 'made available online' for a period of say nine months equivalent to an incident where a film is 'made available online' for a period of one second. This is argued to be a problematic interpretation because, in the context of the BitTorrent protocol, a peer who 'makes a film available online' for one second facilitates far less infringement than the one who 'makes it available online' for say nine months. The applicants therefore argue that there must be a temporal aspect to the 'making available online' copyright act: that is, the longer the film is 'made available online', the greater the number of infringements. They use this as a justification for the DtecNet Agent downloading

a new piece of the file (and therefore alleging a new infringement) every 24 hours from the same IP address (see discussion at [281] of the peer suspension feature of the DtecNet Agent).

292 The Court disagrees with the applicants' submission. The applicants' construction of the term 'make available online' would produce an entirely arbitrary and random result, in respect of the number of copyright infringements. Such conclusion would militate against the construction of the term 'make available online' urged by the applicants. The Court does not accept the further tortured construction whereby, if the IP address remains static and the computer remains connected to the internet, the DtecNet Agent alone decides how many infringements occur. If the DtecNet Agent is designed to download a piece of the file from the same IP address once every 24 hours, it could, for example, connect to the same IP address to download a piece of the file once every 12 hours, or one hour, or five seconds. The mere fact that the DtecNet Agent reconnects only every 24 hours is not evidence of it artificially reducing the number of infringements that could be alleged as was submitted. Rather, it is evidence of the artificiality of the number of infringements being alleged. If the applicants submit that each one of those incidents would constitute a separate incident of 'making available online', the DtecNet Agent could be set up to find thousands of 'make available online' infringements every day if the applicants and AFACT so chose.

293 The issue of the temporal nature of 'making available online' is not something that is relevant only to the BitTorrent system. A person who hosts copyright infringing material on their website for a month facilitates more infringement than one who does so for a day, yet it is not as if such possibility would not have been alive in the minds of the legislative drafters when the communication right was incorporated into the Copyright Act as part of the *Copyright Amendment (Digital Agenda) Act*.

294 The legislature saw fit to formulate the legislation without reference to any temporal aspect such that one makes available online once per calendar day, or month, or year. The provision merely states 'make available online'. In fact, other sections of the Copyright Act suggest that there is no temporal aspect to the phrase 'make available online' in s 10. For example, s 135ZWA(2A) of the Copyright Act (incorporated into the Copyright Act at the same time as the 'make available online' copyright) may be summarised as relevantly stating:

> If…a work is reproduced by…an administering body…and…the reproduction is communicated by…the body by being made available online…and…the reproduction remains available online for longer than the prescribed period; then, when that period ends:…the reproduction…is taken to have been communicated again by…making it available online for a further prescribed period'.

Section 135ZWA(4) defines the '*prescribed period*' as 12 months or as otherwise agreed. The necessity for this imposition of a temporal aspect relating to the 'make available online' act suggests that, absent such imposition, there is no temporal aspect.

295 In neither *Kazaa* nor *Cooper* (at first instance or on appeal in *Cooper v Universal Music Australia Pty Ltd and Others* (2006) 156 FCR 380 ('*Cooper* 156 FCR 380')) where incidences of 'making available online' were found, was there any suggestion that such term ought to have been confined to a set time period, with any continued 'making available online' in excess of that period constituting a new infringement. Contrary to the applicants' oral submissions, neither the Copyright Act, nor any authorities, suggest that a continued 'making available online' infringement evolves into a separate and further infringement if such infringement continues, in the circumstances of these proceedings, after the receipt of an AFACT Notice.

296 The exact moment when the single infringement of 'making available online' occurs under the Court's interpretation of the section is not ascertainable in the abstract because of the manner in which the BitTorrent system operates. Peers share pieces of the film from the moment they receive them. This means that one participates in the swarm from the moment one receives the first piece. However, the Copyright Act focuses on the 'making of the *film* available online' which requires issues related to substantiality in s 14 to be taken into account. That is, in order to infringe, one has to 'make available online' a substantial part of the film.

297 Since the respondent has conceded substantiality in relation to making available online, the Court does not have to engage in an analysis of the issue. In practice, the Court accepts that people seeking to obtain files by means of the BitTorrent system will seek the whole file, and to do so they will have to, at some point, be sharing 100% of the file. At that moment it will be certain that they have 'made the film available online'.

298 The respondent has raised no issue with the films being 'made available online' to the public. It has conceded such issue. Consequently, such issue need not be discussed further.

299 In conclusion, in view of the evidence and of the respondent's concessions, the Court finds that an iiNet user makes *each* film available online *once*. The exact moment when that occurs will vary on a case by case basis, but this is not an issue because the respondent has conceded substantiality in relation to this particular act of infringement.

300 Whatever the frequency of the infringements, the Court finds that, as has been conceded by the respondent, there have been many instances of iiNet users 'making the applicants' films available online' without the licence of the applicants.

'Electronically transmit' a substantial part of the film to the public

301 Similar to the dispute between the parties regarding the 'make available online' act, the parties also have differing interpretations of the act of 'electronic transmission'. The respondent does not concede that the applicants' evidence proves that iiNet users have 'electronically transmitted' films, and provides three reasons. First, it submits that the alleged transmissions do not satisfy the requirement of 'substantial part'; second, the transmissions are not to the public; and third, based upon the respondent's interpretation of the communication right, and leaving aside the evidence of Mr Herps and Mr Fraser, the evidence only discloses that there were communications by the DtecNet Agent, not the iiNet users.

'Substantial part'

302 This proceeding throws into stark relief the difficulty of applying the definition of 'electronic transmission' combined with 'substantial part' with communications which do not occur by means of the traditional client/server model. The evidence establishes that much distribution of data across the internet occurs by means of the client/server model. For example, if http://www.google.com is typed into a computer's web browser, that computer (the client) sends a request to Google's servers (the server), and those servers transmit the requested data to the client, which is interpreted by that web browser as a website.

303 Such communication has two salient features. Firstly, it is between the client and server only. Secondly, all the data sought comes from the server to the client. It appears that the 'electronic transmission' copyright was drafted into the Copyright Act with transmissions of this kind in mind. As has already been explained, the BitTorrent protocol distributes data in a very different manner. There is no central server that provides data to clients; instead all clients are, in effect, servers. There is no one-on-one communication, but rather a multitude of communications between a multitude of computers. The data does not come from one server to the client, rather the data is sourced from many different peers in the swarm.

304 This process gives rise to significant hurdles for the definition of the act of 'electronic transmission' contained the Copyright Act as such act must be done in relation to a substantial part of the film. However, the BitTorrent protocol operates by transmitting thousands of pieces to hundreds of different peers. Each piece is highly unlikely to be a substantial part. A number of pieces are unlikely to be a substantial part. The Court cannot with certainty state whether they would comprise a substantial part in the abstract because substantiality is both a quantitative and qualitative analysis. It would be necessary for the Court to assess each individual allegation of infringement to determine whether or not an infringement occurred, consistent with that which occurred in *TCN Channel Nine Pty Ltd v Network Ten Pty Ltd (No 2)* (2005) 145 FCR 35.

305 The comments made in relation to the *Digital Millennium Copyright Act 1998* (US) ('DMCA') by Ginsburg J in *Recording Industry Association of America Inc v Verizon Internet Services Inc* 351 F3d 1229 (DC Cir 2003) at 1238 ('*Verizon*') are apposite:

> …the legislative history of the DMCA betrays no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works. That is not surprising; P2P software was "not even a glimmer in anyone's eye when the DMCA was enacted."

While his Honour was referring to a specific provision not replicated in the Copyright Act, the comments are apposite to the difficulty in construing the communication right contained in the Copyright Act in regard to p2p systems such as the BitTorrent protocol.

306 The fourth affidavit of Mr Herps includes data which the applicants have consolidated from a number of pieces downloaded by the BitTorrent Agent over a period of many months from the RC-08 subscriber account (one of the RC-20 accounts) in relation to the film

Pineapple Express. The resulting film is viewable for a period of 45 seconds at one point, eight seconds at another point and 47 seconds at another point. The applicants submit that this may well constitute a substantial part of this particular film. The Court observes that the RC-08 account reveals that the film was left available online for some nine months or so which the Court considers was an exceptional period of time on the evidence. Further, such analysis is unnecessary in view of the Court's construction of the 'electronic transmission' act in relation to the BitTorrent system as explained below.

'To the public'

307 The respondent submits there is a question whether these one-on-one (or peer to peer) communications of a single piece of the film satisfy the definition of a communication '*to the public*' as required by s 86(c) of the Copyright Act.

308 The respondent submits that there is a distinction between the communication act of 'making available online', which is conceded in these circumstances to be to the public at large, compared with the act of 'electronic transmission' which, from a technical perspective, is submitted to be in a closed setting to a limited public. The 'electronic transmissions' in this instance are the direct communications between peers in the swarm of pieces of the file. The respondent submits that such communication (being to a limited public) will only constitute a communication to the public within the meaning of that term in s 86(c) if the communication occurs in a 'commercial context', citing *Telstra Corporation Limited v Australasian Performing Right Association Limited* (1997) 191 CLR 140 ('*Telstra v APRA*') at 157.

309 The applicants have provided submissions in support of their contention that this requirement is satisfied. However, the Court finds it unnecessary to determine such issue because of the Court's construction of the 'electronic transmission' being effected in these circumstances, as considered hereunder.

The solution

310 The Court's preference in the circumstances is to take a broad approach. The Court finds that it is the wrong approach to focus on each individual piece of the file transmitted within the swarm as an individual example of an 'electronic transmission'. The BitTorrent system does not exist outside of the aggregate effect of those transmissions, since a person

seeks the whole of the file, not a piece of it. In short, BitTorrent is not the individual transmissions, it is the swarm. It is absurd to suggest that since the applicants' evidence only demonstrates that one piece of a file has been downloaded by the DtecNet Agent from each iiNet user (in some cases more than one, but not many more), the applicants cannot prove that there have been 'electronic transmissions' by iiNet users of the applicants' films. But it is equally absurd to suggest that each and every piece taken by the DtecNet Agent from an iiNet user constitutes an individual 'electronic transmission' infringement.

311 The correct approach is to view the swarm as an entity in itself. The 'electronic transmission' act occurs between the iiNet user/peer and the swarm, not between each individual peer. One-on-one communications between peers is the technical process by which the data is transferred, but that does not mean that such level of detail is necessarily what the communication right in s 86(c) focuses upon. While the DtecNet evidence cannot prove directly that an iiNet user has 'electronically transmitted' a film to the swarm (it can only show that the data has been 'electronically transmitted' to the DtecNet Agent acting as a peer in the swarm) the evidence is sufficient to draw an inference that in most cases iiNet users have done so.

312 It is possible, for example, in situations where the iiNet user obtains the whole of the file (by downloading) without sharing the same amount of data back (by uploading) into the swarm, that the iiNet user might not 'electronically transmit' enough data to the swarm to constitute a substantial part. However, the Court assumes that the viability of swarms relies on peers providing at least as much data as they take, so it can be assumed that peers not transmitting a substantial part of a film to the swarm must be the exception rather than the norm. Consequently, the Court finds that iiNet users have infringed by 'electronically transmitting' the applicants' films to the swarm.

313 In answer to the respondent's submission that the 'electronic transmission' right has not been interpreted in this manner previously, the Court observes that such right has never been the subject of such detailed judicial consideration on any prior occasion. But, more importantly, there is a difference between the technical process by which an 'electronic transmission' occurs and the copyright act of 'electronically transmitting'. That is, there is a difference between the process of electronic transmission and the legal definition of that term.

314 For example, in the case of a simple transmission between a client and server, it must be remembered that it is in the very nature of the internet (as described at [44]-[48] of this judgment) that the transmission of data is effected by means of that data being broken up into thousands or millions of tiny packets of data, which are then individually routed, not necessarily along the same path, between the server and the client. Each of these packets cannot possibly be a substantial part of a film. Yet, if the focus was at this level of detail, it would be impossible for an 'electronic transmission' (in the s 86(c) sense) to *ever* occur, because the transmission of files would actually be seen as a series of 'electronic transmissions', each of which are insufficient to constitute a substantial part. Given that the communication copyright was drafted with the internet in mind (see the objects to the *Copyright Amendment (Digital Agenda) Act*), and one would assume that it was intended that it be possible for an infringement to occur by means of an 'electronic transmission' over the internet, the assumption arises that for infringement purposes, the focus need not be on the precise technical means by which a communication occurs, but rather upon the substantive effect of a communication.

315 Such interpretation has much to commend it. It overcomes the hurdle of 'substantial part' being an issue. However, it also obviates a second issue, namely whether the communication is made 'to the public'. If the swarm is seen as the aggregate, rather than each individual peer within it, it is clear that the communication is to the public for the same reason that the respondent concedes that iiNet users 'make available online' to the public. That is, the communication is made to the public at large. On the evidence before the Court, swarms for popular files (which the applicants' films frequently are) often contain many thousands of peers. Any one or a number of those peers are able to receive pieces of a film from an iiNet user participating as a peer in the swarm. BitTorrent works because there is an underlying assumption that every peer is willing to share with every other peer. Generally there are no restrictions on entry to a swarm, other than finding the relevant .torrent file. Consequently, a communication to the swarm cannot be seen as anything other than a communication to the public.

316 One issue arises from the Court's interpretation of the 'electronic transmission' act in regards to the BitTorrent protocol and it is a similar one to that discussed in relation to the 'making available online' copyright. The issue is whether the 'electronic transmission'

between the iiNet user and the swarm is one transmission, or whether it could be multiple transmissions, each constituting a single infringement. For the reasons outlined above at [312], the Court assumes that, in most circumstances, an iiNet user will transmit back to the swarm at least a substantial part of the file, more likely 100% of the file so as to ensure that the iiNet user uploads as much as was downloaded. The question then remaining is whether, if one was to transmit more than 100% of the file back to the swarm, that would constitute more than one infringement.

317 As with its finding in relation to 'make available online', the Court finds that the term 'electronically transmit', in relation to the BitTorrent system cannot be seen as a series of single acts. BitTorrent use is an ongoing process of communication for as long as one wishes to participate. Therefore, the term 'electronically transmit' cannot sensibly be seen in that context as anything other than a single ongoing process, even if the iiNet user transmits more than 100% of the film back to the swarm. Once the hurdle of 'substantial part' is overcome initially, that is, the iiNet user transmits a substantial part, there is no more than one infringement, whether the iiNet user transmits the whole of the data making up a film back into the swarm or more than that amount of data. Therefore, similarly to the Court's finding regarding 'making available online' (and again leaving aside the exceptional instance of a person seeking to transmit the same film repeatedly via the BitTorrent system which is not suggested here), it finds that *each* iiNet user 'electronically transmits' *each* film *once*.

318 The respondent also raises an issue regarding the requirement that the infringing act must, pursuant to s 101, occur in Australia. Since the 'electronic transmission' of data to the swarm by iiNet users does take place from Australia, this requirement is satisfied.

Who makes the communication?

319 Such finding does not completely answer the issues raised in relation to 'electronic transmission' act, as the respondent raises a final issue regarding who it is that makes the communication.

320 The respondent submits that in the case of the DtecNet evidence, the communications are made by the DtecNet Agent, not the iiNet user, with the consequence that the DtecNet

Agent is one who 'electronically transmits' within the meaning of that term in s 10 of the Copyright Act.

321 Further, the respondent submits that Mr Herps and Mr Fraser have been licensed by the applicants and therefore their actions cannot be treated as infringements. The respondent submits that for this reason there is no evidence before the Court of any infringing 'electronic transmissions' by iiNet users. The Court will address first the communication issue, then the licence issue.

322 The relevant section of the Copyright Act which bears upon this issue is s 22. Section 22 states:

> …
>
> (6) For the purposes of this Act, a communication other than a broadcast is taken to have been made by the person responsible for determining the content of the communication.
>
> (6A) To avoid doubt, for the purposes of subsection (6), a person is not responsible for determining the content of a communication merely because the person takes one or more steps for the purpose of:
>
> (a) gaining access to what is made available online by someone else in the communication; or
>
> (b) receiving the electronic transmission of which the communication consists.
>
> Example: A person is not responsible for determining the content of the communication to the person of a web page merely because the person clicks on a link to gain access to the page.

Subsection (6) was discussed in *Cooper* 150 FCR 1 at [69]-[76] and briefly at [362] in *Kazaa*.

323 The disagreement between the parties relates to their alternative characterisations at a technical level of how each communication of a piece of the file between peers is effected by the BitTorrent protocol.

324 As already mentioned, the Court does not consider the relevant 'electronic transmission' to be the transmission of each piece of a film between an iiNet user and a peer in the swarm, but rather between the iiNet user and the swarm itself. Consequently, the issues arising regarding the person who makes or originates the communication do not arise under the Court's construction of the 'electronic transmission' right in the present circumstances. It

is clear that the person responsible for determining the content of the communication is the iiNet user who chooses a particular .torrent file, connects to that swarm, and, over time, 'electronically transmits' to that swarm the file as they themselves receive pieces of it. The effect of s 22(6A) would appear to be that the iiNet user cannot be said to 'electronically transmit' if they receive data *from* the swarm. However, as has been made clear, the 'electronic transmission' is from the iiNet user *to* the swarm.

325 There is no direct evidence of the transmission of data to the swarm as a whole, as the evidence before the Court is of transmission of and logging of data between the iiNet user and the DtecNet Agent. However, the Court finds that such evidence, coupled with the evidence of the operation of the BitTorrent protocol and with the Court's interpretation of 'electronically transmit' in the current context, is sufficient to draw an inference that there is an 'electronic transmission' by iiNet users to the swarm, and that such transmission is infringing the applicants' copyright.

Were the applicants' investigators licensed?

326 The relevance of much of the debate regarding who 'electronically transmits' pursuant to s 22(6) stems from the respondent's contention that the applicants' investigators, Mr Herps and Mr Fraser, were not infringing the copyright of the applicants because they were licensed by the applicants to do copyright acts in relation to the films. The Court's analysis of the term 'electronically transmit', in particular in relation to s 22(6) and (6A) of the Copyright Act, makes the debate redundant because the Court does not need the evidence of Mr Herps or Mr Fraser to conclude that iiNet users 'electronically transmitted' films: the DtecNet evidence is enough. However, given that licence was a highly contested issue the Court will consider the submissions of both parties.

327 As established in *Avel Proprietary Limited v Multicoin Amusements Proprietary Limited and Another* (1990) 171 CLR 88, it is for the applicants to prove that particular infringements occurred in the absence of their licence. Such proposition is, in itself, a tautology. If licence exists there could be no infringement since the absence of licence is a precondition to an infringement of copyright. The respondent has conceded that where the applicants can prove a copyright act committed by iiNet users, such act was an infringement because it occurred without the licence of the applicants. However, the respondent does not

concede that Mr Herps and Mr Fraser (who were both employees of AFACT and subscribers of the respondent) were unlicensed by the applicants when they downloaded the applicants films via the respondent's internet service as subscribers of the respondent.

328 In the Full Federal Court decision of *Computermate Products (Aust) Pty Ltd v Ozi-Soft Pty Ltd and Others* (1988) 20 FCR 46 Sheppard, Spender and Gummow JJ found that the word 'licence' in s 37 of the Copyright Act was interchangeable with the words 'permission' or 'consent' (at 48-49). Their Honours also found that a licence did not have to be brought about by means of a contract: rather, a 'bare' licence could be inferred from factual circumstances (at 49-50 and 51). The Court can find no reason not to interpret the word 'licence' in s 101 of the Copyright Act in the same manner as s 37 of the Copyright Act. Consequentially, the Court considers that the words 'licence', 'consent' or 'permission' are interchangeable in s 101 of the Copyright Act.

329 The applicants rely upon two pieces of evidence supporting their contention that there was no licence, namely the statements of the studio executives and the evidence of Mr Gane. Each will be dealt with in turn.

STUDIO WITNESSES' EVIDENCE

330 The applicants firstly refer to statements in each of the studio witnesses' affidavits as evidence of the absence of licence in relation to the AFACT investigators, Mr Herps and Mr Fraser. Those statements, which are substantially identical, are in very broad terms. For example, Ms Garver of NBC Universal stated:

> From my own knowledge and my review of the books and records of Universal, I confirm that the Universal Applicants and their licensees have not given any licence, permission or consent:
>
> (a) to any customers of the respondent (**iiNet Customers**) or persons accessing the internet by means of the internet accounts of iiNet Customers, to make available online or electronically transmit in Australia (including by means of BitTorrent technology), or make copies in Australia of, the whole or a substantial part of any of the motion pictures or television programs contained in the Universal Film Catalogue, including the Universal Films…

331 As a matter of common sense, this statement cannot do what the applicants wish it to do. It seeks to speak for both the Universal applicants and all their licensees and is said to relate to all iiNet users. This cannot be correct. For example, iTunes must be a licensee of

some of the applicants. As discussed at [184] it provides the means by which people can purchase and download films of the applicants to their computers (among other things) and that download necessarily involves making a copy of a film (for the same reason as downloading via the BitTorrent system). The evidence at [184] also establishes that iTunes is widely used by iiNet users. Therefore, was Ms Garver's statement or any of the other studio witnesses' statements correct, iiNet users who purchased and downloaded copies of the applicants' films legitimately through iTunes would infringe copyright, because they were never granted a licence by any of the applicants or their licensees to do so. This is obviously incorrect.

332 As the iTunes Store Terms of Service (exhibit N) states of purchases from the iTunes Store:

> 10. b. Use of Products
>
> Usage Rules
>
> …
>
> (iii) Your licence of Products as authorised hereunder permits you to use the Products on five iTunes-authorised devices at any time…
>
> (iv) You shall be able to store Products from up to five different Accounts on certain devices…at any time.
>
> …
>
> (vii) You shall be entitled to export, burn (if applicable) or copy (if applicable) Products solely for personal, non-commercial use.

Each of these devices (for example, '*an iPod, iPhone or Apple TV*') will require a copy of the film to be placed on it to enable legitimate use, thus the licence necessarily extends to making a copy of the film within the meaning of s 86(a) of the Copyright Act. Therefore, assuming that iTunes itself is ultimately licensed by the Universal applicants (which one assumes it must be because Mr Dalby gave evidence of the availability of Universal films to download from iTunes) iTunes would then licence any person, including an iiNet user, who purchased one of the Universal films through iTunes to make a copy of it. The Court assumes that at least some iiNet users have purchased the Universal films through iTunes. This is in direct contradiction to Ms Garver's statement that '*I confirm that the Universal Applicants and their licensees have not given any licence…to any customers of the respondent…or persons accessing the internet by means of the internet accounts of the iiNet Customers, to…make*

copies in Australia of…any of the motion pictures or television shows contained in the Universal Film Catalogue'. In the circumstance of such contradiction, the Court finds that the statement of Ms Garver at [330] and any similar statement of the other studio witness to be unreliable.

333 Further, as already found, a licence need not be formal or contractual. It can be implied from conduct. It can be entirely casual. Therefore, it is unlikely in this circumstance that the books and records of Universal, or of any other studio for that matter, would provide any guidance as to whether Mr Herps and Mr Fraser were licensed to do what they did. The Court accepts the broad accuracy of statement extracted above of Ms Garver, and statements of other studio witnesses to the same effect, but they cannot, by themselves, prove absence of licence in circumstances where other evidence suggests that licence exists, as the preceding discussion in relation to iTunes has shown.

MR GANE'S EVIDENCE

334 Mr Gane answered, in reply to a question asked of him whether his investigators had the licence of the copyright owners, '*of course not*'. He stated that '*[t]here may be occasions where my investigators – I actually direct them and instruct them, which you may technically say is infringement of copyright, when they go out and purchase, or download pirated copies. It is an investigative technique*'. With respect to Mr Gane, such statements reflect a layperson's understanding of copyright law. Copyright is not infringed by purchasing an infringing copy (the infringer is the person who creates that copy), but that is immaterial. More importantly, one does not '*technically*' infringe copyright. Either copyright is, or is not, infringed. If a licence exists, no infringement can occur. Whilst Mr Gane understood that there was no licence, the Court considers that this understanding was made on a far too narrow and formal interpretation of the word 'licence'. Licence can be inferred and it can be inferred *by conduct*. Just because Mr Gane may have thought that he was ordering the infringement of copyright does not mean that he was. Regardless, as will be shown, Mr Gane's own evidence contradicts his belief. There is ample evidence, as detailed hereunder, sufficient to establish that the AFACT investigators were, in fact, licensed by the applicants to do copyright acts in relation to the films.

335 As already discussed above at [82], AFACT is affiliated with the MPA, which is the primary industry body of the applicants. In practical terms, AFACT is the local 'franchise' of the MPA. AFACT receives its funding from the applicants. Mr Herps and Mr Fraser are employees of AFACT. While the evidence suggested that the studios provided funds to AFACT but were largely 'hands off' in relation to the operation of AFACT, this does not lead to the conclusion that there was not an implicit licence given to AFACT to use the applicants' films as necessary for the purposes of gathering evidence for investigations of infringement and litigation. It seems most unlikely that the applicants would provide money to an organisation for the purpose of knowingly infringing their copyright. One might argue that such money was provided in order for AFACT to infringe copyright for the purposes of preparing for litigation or investigation of copyright infringement, but such reasoning is circular. If funding was provided in order to gather evidence for the purposes of a proceeding or for other reasons, that is evidence that there was permission or consent for Mr Herps and Mr Fraser to do copyright acts. One cannot give permission for one's copyrights to be infringed; the very granting of permission vitiates the infringement, because the infringement is predicated on the absence of permission.

336 Indeed, it is this aspect which exposes the fallacy of the applicants' position. The cross-examination of Mr Gane and Mr Herps establishes that no films were downloaded or were directed by Mr Gane to be downloaded via the BitTorrent system by Mr Herps and Mr Fraser (and consequently no further copies of such films were made on DVD or other media) until those films were included in a list of films prepared by the applicants that were '*cleared for litigation*'.

> [Mr Gane]: But the details [of the AFACT investigations], by and large, are left up to you and to AFACT?---The details, in terms of how to conduct the investigation, would be up to me.
>
> Thank you. In this case, there were some details that were given to you from either the regional office or the head office, such as, for example, the list of titles approved for Australian litigation, correct?---Correct.
>
> …
>
> Thank you. And those activities that he [Mr Herps] engaged in…they were part of his duties as an employee of AFACT?---They were part of his instructions to – from myself, to be an – as part of his investigative capabilities, so yes.
>
> Yes. And he downloaded the films that you told him to download?---No.
>
> Did he download titles that had been put onto the studio lists, cleared for litigation in

> Australia, as we discussed earlier?---Some of the titles, yes.
>
> …
>
> And he [Mr Fraser] did those activities, as directed by you?---Yes, he did.
>
> …
>
> [Mr Herps]: …And during that period, 19 to 27 June 2008, you downloaded some films via BitTorrent, is that correct?---That's correct.
>
> And was that on the instructions of Mr Gane?---Yes, it was.
>
> And were you informed which titles of films you should seek to download in the course of that process?---Not directly which titles, but any number of titles.
>
> …
>
> And you searched for files containing copies of six motion picture television programs you list, there. Is that a list of titles or episode names that were identified to you by Mr Gane that you should look for?---They were part of a series.
>
> Yes. So he identified more titles than that and these were among them?---Yes.
>
> And were you acquainted, by 27 June 2008, with a procedure that might be described as the DtecNet evidence gathering procedure?---Yes.
>
> Thank you, and did that involve engaging in activities that were directed at titles that came from a list of clear titles that had been added to something called share point?---That's correct.
>
> And you confide [sic-likely confine] yourself with the stage of the activities to the titles that were so cleared and available on share point?---That's correct.

Such studios' list was regularly updated by the applicants on Microsoft SharePoint (which is a secure online facility for the MPA and affiliates to share content). That is, the copyright owners or exclusive licensees were the bodies that generated those lists. The act of placing those films in the '*cleared for litigation*' list is sufficient evidence to imply that the investigators where then licensed to do copyright acts in relation to them. Only by undertaking the investigations could evidence be obtained for the litigation. Mr Perry of Paramount, for example, said:

> And so, from when the title was put on SharePoint, you understood that that was a title that would be the subject of the sorts of investigations that DtecNet was carrying out; correct?---Yes
>
> And the subject of the sorts of activities that AFACT was carrying out; is that correct?---Yes

337 To find further evidence of licence one need only look at the fact that Mr Herps and Mr Fraser have voluntarily submitted affidavit evidence before the Court of actions which,

but for a licence from the applicants, would constitute copyright infringement. The damages for such copyright infringement could be substantial, and one might suggest the word 'flagrant' within the meaning of that term in s 115(4)(b)(i) of the Copyright Act applies to such conduct, given its blatant and open nature, such that it would satisfy an award of additional damages. It could scarcely be accepted that Mr Herps and Mr Fraser would volunteer to perform such acts if they did not know implicitly or explicitly that the applicants would not bring suit against them to seek damages for copyright infringement in the circumstances where they delivered themselves before the Court with evidence of such copyright infringement. Further, the applicants have not moved against them since such evidence was read and admitted before the Court. When all these circumstances are considered, the Court does not accept the width of what is relied upon by the statements of the studio executives or Mr Gane. Their understanding is negatived by the contradictory evidence.

MOORHOUSE

338 The applicants submit that the present circumstances are similar to the events occurring in *The University of New South Wales v Moorhouse and Another* (1975) 133 CLR 1 ('*Moorhouse*'). In that case a university graduate, Mr Brennan, presumably prompted by, or at the request of, the Australian Copyright Council (said to have '*instigated, or at least supported*' the proceedings (at 7)) supplied the evidence of primary infringement by copying pages out of a book (discussed in more detail below at [368]). In that case, it was found that such act was an infringement of copyright by Jacobs J (with McTiernan ACJ agreeing) at 20 and Gibbs J at 11.

339 The Court does not consider that *Moorhouse* stands for any broad proposition that deliberate actions taken by investigators for the purposes of litigation constitute infringement of copyright.

340 Furthermore, *Moorhouse* is readily distinguishable. There does not appear to have been any argument in that proceeding as to the existence or absence of licence of the primary infringer. Since the proceeding was clearly a 'test case' (see [367] below) regarding *authorisation*, no occasion arose to consider any issue of licence. Both Gibbs J and Jacobs J turned their minds only to whether the act of photocopying was a copyright act, whether it

was done in relation to a substantial part of the work and whether there was any statutory defence. Consequently, it is not surprising that their Honours did not turn their minds to the question of licence. As their Honours Gleeson CJ, Gummow and Heydon JJ stated in *CSR Limited v Eddy* (2006) 226 CLR 1 at [14]:

> But where a proposition of law is incorporated into the reasoning of a particular court, that proposition, even if it forms part of the ratio decidendi, is not binding on later courts if the particular court merely assumed its correctness without argument…

341 The Court notes that the issue of licence was discussed in the first instance judgment in *Moorhouse & Angus and Robertson (Publishers) Pty Ltd v University of New South Wales* (1974) 3 ALR 1 ('*Moorhouse* 3 ALR 1') at 15. However, it is important to distinguish such decision on two grounds. Firstly, the first instance judge only analysed whether licence was extended to Mr Brennan from Angus and Robertson (the publisher of Mr Moorhouse's work) pursuant to a specific clause of an agreement between Angus and Robertson and Mr Moorhouse which was not reproduced in the primary judgment. Accordingly, the terms of such agreement are unknown. Secondly, Angus and Robertson provided no evidence in those proceedings. Therefore, the Court does not consider the primary judgment's discussion of licence to be a discussion of licences in such scenarios generally. Rather, it was specific to the factual circumstances of those proceedings and those circumstances are distinct to those in the present circumstances.

342 Further, there is clearly a far higher degree of awareness on the part of the studios of the general actions of AFACT than there was from the copyright owner in *Moorhouse*, who was found to '*not know beforehand that it was proposed to make a copy of part of his book*' (see Gibbs J at 7-8). Ms Garver, for example, may not have personally known that Mr Herps personally would be undertaking copyright acts, but that is hardly surprising. The applicants knew, at least in general terms, what was occurring. Finally, it is not certain whether Mr Moorhouse had any association with the Australian Copyright Council, the body that appears to have prompted the proceedings in *Moorhouse*. In the present proceedings the applicants have delegated some investigations of the infringement of their copyright to AFACT.

343 It is for the applicants to prove there was no consent, licence or permission for Mr Fraser and Mr Herps to undertake acts comprised in the applicants' copyright. The applicants have not so satisfied the Court. Indeed, the Court is positively satisfied that there *was*

consent, licence or permission for the copyright actions undertaken by Mr Herps and Mr Fraser.

344 Despite such finding, the Court does not find the issue to be of any real consequence. Whether or not Mr Herps and Mr Fraser were licensed matters little for two reasons. Firstly, it is always open to the Court to infer from actions which are licensed that actions which are not licensed are occurring. Secondly, and more importantly, the Court does not rely on the evidence of either Mr Fraser or Mr Herps for any of the infringements found to have been proven by the applicants above. That evidence is provided by DtecNet. As already found, when one considers the DtecNet evidence as being evidence of the likelihood that an iiNet user has 'electronically transmitted' the film to the swarm, rather than 'electronically transmitted' a piece of the film to the DtecNet Agent as a peer, it is immaterial whether the investigator such as DtecNet is or is not licensed. Further, as will become apparent from the discussion below, whether or not Mr Herps or Mr Fraser were licensed has no impact on the Court's finding in relation to whether the applicants have made out their claim that iiNet users have made further copies of films onto other storage media.

Did s 104 of the Copyright Act apply?

345 The respondent pleaded that the actions of Mr Herps, Mr Fraser and DtecNet were also done for the purpose of this proceeding and thus attracted s 104 of the Copyright Act which states that copyright is not infringed where a copyright act is done '*for the purpose of a judicial proceeding*'. However, the respondent made no mention of such argument in its closing submissions and the Court considers that it was abandoned. Even if not abandoned, the Court rejects it. The Court believes that the scope of s 104 is narrow, similar to s 45(1) of the *Copyright, Designs and Patent Act 1988* (UK) and thus would not cover the actions undertaken by Mr Herps, Mr Fraser or DtecNet. Regardless, the issue is irrelevant as the Court has found that the activities of Mr Herps and Mr Fraser were non-infringing because they had the licence of the applicants.

Make a copy of a substantial part of a film

346 The final type of infringement alleged by the applicants is that iiNet users have made copies of the applicants' films. There are two types of copies alleged to have been created. The first are the copies of the films necessarily created by the iiNet users upon downloading a

file from a swarm, namely the very file sought by the iiNet user from a swarm is an infringing copy. The applicants also allege that iiNet users have then made subsequent copies on physical media such as hard drives, DVDs or other storage media from the copy downloaded from the BitTorrent swarm. The Court will deal with each alleged infringement in turn.

Copies from BitTorrent

347 The respondent admits that where the applicants' evidence shows a particular iiNet user sharing a file with a swarm, it is highly likely that that iiNet user obtained that copy from the swarm, and it is therefore an infringing copy. Accordingly, there is no real dispute between the parties that iiNet users have made infringing copies of the applicants' films. After all, obtaining a copy of the film is the whole reason that iiNet users would infringe the applicants' copyright in the first place. An iiNet user derives no benefit from 'making available online' the film to the swarm, nor 'electronically transmitting' the film to the swarm (except in the sense that these actions are preconditions for participation in the swarm). These actions are merely consequential effects of the iiNet user's actions in obtaining, for personal use, an infringing copy of the film. Further, the fact that the file being shared with the swarm has the same hash value as the file being shared in that particular swarm means that it is essentially impossible for the film to have been sourced from anywhere else, or to be a legitimate copy.

348 The respondent submits as a possibility that the copy may have been obtained from the swarm at a time while the particular computer in question was connected to the internet via a different ISP (such as laptop used at work and at home). However, as the respondent also admits, this is nothing other than a possibility.

Further copies made on physical media

349 The applicants' further claim, namely that iiNet users made further copies on physical media (such as a DVD) for viewing for other purposes, is infringement one step removed from those outlined above because the alleged infringement does not take place across the respondent's facilities. This particular claim was the subject of a strike-out motion in *Roadshow No 1* and at [33]-[34] the Court refused such motion. However, in the Court's refusal to strike-out the claim, the Court stated that '*the Court is mindful that if the evidence*

of Roadshow [the applicants] proves inadequate to satisfy the requisite burden of proof, such claim will fail'.

350 The only admissible evidence supporting such claim is the actions of Mr Herps and Mr Fraser, an affidavit by Mr Gane and documents regarding an AFACT criminal copyright infringement investigation. The Court concludes that such evidence establishes that it is a technical possibility that further copies are being made. But such evidence can give absolutely no guidance to the Court how frequently such action occurs, or how likely it is to occur. In summary, the evidence only raises the possibility that further copies are being made.

351 The actions of Mr Herps and Mr Fraser show the technical capability of such subsequent copying. However, as Mr Herps and Mr Fraser acted in order to gather evidence solely for the purposes of investigation of copyright infringement and eventually these proceedings, the Court is circumspect in accepting their evidence as objective evidence of the propensity of certain actions undertaken by iiNet users. The Court would make such finding irrespective of whether they were licensed.

352 Brief evidence was given of an investigation conducted by AFACT known as the AFACT 'Rama' investigation into the copyright infringement of certain individuals who subscribed to iiNet (not related to these proceedings). Such investigation concerns commercial-scale criminal copyright infringement, for which individuals have been charged. The Court has been informed by the applicants that such persons charged are presently before the Local Court in Brisbane. The Court finds that such conduct is unlikely to be typical of an iiNet user. Indeed, much of the applicants' submissions, particularly in criticism of the respondent's practice of forwarding the AFACT Notices to the police, are predicated on an assumption that the actions of the infringing iiNet users are not criminal actions.

353 The Court does not consider the opinion of Mr Gane that it is '*likely*' that further copies would be made on DVD or other storage material to be sufficient evidence of the likelihood of that conduct in relation to iiNet users. Mr Gane appears to deal mainly with commercial-scale infringements. The Court made clear that while the evidence of Mr Gane on this issue would be admitted, its relevance and weight would be minimal.

354 Finally, in relation to the piracy reports exhibited to the first affidavit of Mr Gane, the Court can find no guidance from such reports. The reports in question are general reports relating to worldwide copyright infringement trends and studies of general internet traffic. The applicants have not pointed to any particular sections of such reports as providing evidence of the likelihood of films downloaded from the internet being further copied onto other storage media, let alone by iiNet users.

355 The Court does not believe that such evidence is sufficient to prove that, on the balance of probabilities, iiNet users have made further copies of the applicants' films on DVD or other storage media. Upon the evidence before it, the Court does not find that such infringement is made out.

Conclusion

356 The Court finds that iiNet users have 'made available online', 'electronically transmitted' and made copies of the applicants' identified films without licence of the applicants (except in the case of Mr Herps and Mr Fraser). The Court does not find that iiNet users have made further copies on other storage media. Therefore, the applicants have proven primary infringement on the part of the iiNet users, and consequentially the next step is for the Court to consider whether the respondent can be said to have authorised those acts.

PART E1: AUTHORISATION

357 The key issue in these proceedings is that of copyright authorisation. Primary infringement has been established in Part D. Therefore, the next question the Court must consider is, pursuant to s 101 of the Copyright Act, whether the respondent *authorised* the doing in Australia of any act comprised in the copyright of the applicants by those that have been found to have infringed.

358 In the 1987 decision of *Hanimex*, Gummow J commented at 285 that '*[t]he evolution of the meaning of "authorisation" in the 1911 Act and the 1968 Act has pursued perhaps an even more tortuous course than the doctrine of contributory infringement in the United States*'. The Court concurs with such statement, and it has become even more apt in the years following that decision. Despite the legislature's attempt to simplify the relevant considerations pursuant to the *Copyright Amendment (Digital Agenda) Act* and s 101(1A), the

law of authorisation has continued to grow more complicated and unwieldy, with a litany of competing and contrasting considerations, and with one statement of principle frequently matched with a contradictory one. The authority on authorisation has become a mire. There seems to be little certainty other than the basic maxim that authorisation is a question of fact to be decided in the particular circumstances of each case: see *Performing Right Society, Limited v Ciryl Theatrical Syndicate, Limited* [1924] 1 KB 1 at 9; *The Corporation of the City of Adelaide v The Australasian Performing Right Association Limited* (1928) 40 CLR 481 at 504 (‘*Adelaide Corporation*’); *Moorhouse* at 21; *Australasian Performing Right Association Limited v Jain* (1990) 26 FCR 53 at 59 (‘*Jain*’); *Australasian Performing Right Association Ltd v Metro on George Pty Ltd and Others* (2004) 61 IPR 575 at [17] (‘*Metro*’); *Nominet UK v Diverse Internet Pty Ltd and Others* (2004) 63 IPR 543 at [129] (‘*Nominet*’); and *Cooper* 150 FCR 1 at [80]; *Kazaa* at [368].

Judicial consideration of authorisation

359 In the following discussion a number of authorisation decisions will be considered. However, the Court considers that four specific decisions must be considered in greater factual detail. They are *Moorhouse*, *Kazaa*, *Cooper* 150 FCR 1 and *Cooper* 156 FCR 380. *Moorhouse* is discussed in detail in the section regarding the ‘means’ of infringement. The other three decisions will be considered below.

Kazaa

360 The information underlying the following discussion is sourced from [59]-[61] of *Kazaa*. The *Kazaa* proceedings dealt with computer software known as the Kazaa Media Desktop. This software allowed a person to access, via the internet, two networks known as FastTrack and Joltid PeerEnabler. The Court will refer to the software and networks together as the ‘Kazaa system’. By means of the Kazaa system users could search for files contained in the computers of other users on the system. Once files of interest were found, the users could connect directly to the computer containing those files and download the file. This is similar, at least in substantive effect, to how the BitTorrent system operates. However, there are important technical differences between the technologies. The Kazaa system had, according to the applicants in those proceedings, ‘*P2P characteristics [however] it is now clear that it has many features in common with client/server and centrally indexed systems*’.

The BitTorrent system appears to have more p2p characteristics than client/server characteristics.

361 The individuals and corporate entities responsible for the creation and maintenance of the Kazaa system were sued for authorisation of the copyright infringement of the users of the Kazaa system.

362 Wilcox J found that the respondents had authorised the offending conduct. In particular, his Honour found at [489] that Sharman and Altnet authorised the infringements which resulted from the use of the Kazaa system, both entities responsible for the creation and maintenance of the Kazaa system. His Honour found at [411] that by means of technical mechanisms, namely 'keyword filtering' and the 'gold file flood', the respondents had the means to prevent or at least substantially reduce the number of infringements which were occurring by use of the Kazaa system. His Honour found at [404] that it was in the respondent's financial interest for there to be ever increasing amounts of file-sharing and the respondents knew that copyright infringement was the predominant use of the Kazaa system. Further, his Honour found at [405] that the respondents had positively exhorted or encouraged users of the Kazaa system to infringe copyright: that is, it was the intention of the respondents that the Kazaa system be used to infringe copyright.

Cooper

363 *Cooper* 150 FCR 1 concerned the operation of the website at http://www.mp3s4free.net which was created by Mr Cooper. At [84] Tamberlin J found that the website was highly structured and user-friendly and contained hyperlinks to other websites, or remote servers, which contained music files. Therefore, a person who visited Mr Cooper's website was provided with the means to quickly and easily download copyright infringing music files, although those files were not directly hosted on Mr Cooper's website. On appeal in 156 FCR 380 it was admitted by Mr Cooper at [2] that the overwhelming majority of hyperlinks on his website went to copyright infringing music files.

364 Tamberlin J found in *Cooper* 150 FCR 1 at [84] that Mr Cooper intended and designed his website to be used for copyright infringement. Tamberlin J found at [88] that Mr

Cooper authorised the copyright infringement that resulted by use of his website. Such findings were upheld on appeal in *Cooper* 156 FCR 380.

365 Mr Cooper's website was hosted by an ISP known as E-Talk/Com-cen ('Comcen'). Tamberlin J found at [122] that Mr Cooper was actively assisted in the creation of his website by an employee of that ISP. It was also clear to Tamberlin J at [119] that Comcen was well aware of the copyright infringing nature of Mr Cooper's website. Comcen had in fact made an arrangement with Mr Cooper whereby Mr Cooper's website would be hosted free of charge in exchange for Mr Cooper advertising Comcen's services on his website (at [36]). Tamberlin J at [117] found such an arrangement was unlikely to have been made unless Comcen stood to make a commercial benefit, and it would only have known that it stood to make a benefit if it was aware of the high volume of traffic going to Mr Cooper's website and its copyright infringing nature. Finally, Tamberlin J found at [121] that Comcen had the power to prevent the infringements occurring by means of Mr Cooper's website by refusing to continue to host it. These findings were upheld on appeal in *Cooper* 156 FCR 380 by Branson J and Kenny J in separate judgments, with French J (as he then was) agreeing with both decisions.

366 These decisions, and the factual circumstances particular to them, will be referred to throughout this part of the judgment.

The 'means' of infringement

Moorhouse

367 In an uncharacteristic lack of prescience, Gibbs J said at 12 of the *Moorhouse* proceedings '*[i]t will be seen that the present appeal, although intended to be a test case, is of limited significance*'. Judicial history has proven otherwise. The Full Federal Court decision of *Jain* at 57 stated '*[t]he starting point [of an analysis of authorisation] is the Moorhouse case*'. The Court agrees and considers that it remains so following the insertion of s 101(1A) into the Copyright Act. That section does not change the role of *Moorhouse* as '*s 101(1A) is premised on the concept of "authorization" developed by the High Court in that case*' (per Kenny J in *Cooper* 156 FCR 380 at [136]): see also *Kazaa* at [402]; and *Cooper* 150 FCR 1 at [83].

368 As discussed, *Moorhouse* considered the factual circumstance of coin-operated photocopiers provided by the University of New South Wales ('the university') in its library. Mr Brennan copied a short story out of a copyright work, specifically the book '*The Americans, Baby*'. At first instance it was found that Mr Brennan had infringed copyright. However, the university was not found to have authorised Mr Brennan's infringement given that it did not '*induce*' him to infringe: see *Moorhouse* 3 ALR 1 at 15. On appeal, both Gibbs J and Jacobs J (with McTiernan ACJ agreeing) found that the university had infringed. Their Honours, while agreeing on the outcome, each approached the issue on a slightly different line of reasoning.

GIBBS J

369 Gibbs J found at 12, adopting *Adelaide Corporation* and *Falcon v Famous Players Film Company* [1926] 2 KB 474 ('*Falcon v Famous Players*'), that the word 'authorise' means '*sanction, approve, countenance*' and can also, pursuant to *Adelaide Corporation*, mean '*permit*'. His Honour found at 12 that one cannot be said to authorise the infringement of copyright unless one has some power to prevent it, citing *Adelaide Corporation*, and that express or formal permission or sanction is not necessary in that inaction or indifference can reach a degree whereby authorisation will be inferred, again citing *Adelaide Corporation*. While indifference can lead to authorisation, his Honour stated at 12 that authorisation requires a mental element such that it will not be found where one is inactive and does not know or have reason to know that infringements are occurring, pursuant to *Adelaide Corporation*. His Honour then said, in perhaps the most cited encapsulation of the requirements of authorisation (at 13):

> It seems to me to follow from these statements of principle that a person who has under his control the means by which an infringement may be committed – such as a photocopying machine – and who makes it available to other persons knowing, or having reason to suspect, that it is likely to be used for the purpose of committing an infringement, and omitting to take reasonable steps to limit its use to legitimate purposes, would authorize any infringement which resulted from its use.

370 The first consideration, therefore, was whether the university had provided the 'means' by which an infringement may be committed. On the facts before him, his Honour noted at 13 that the university made available '*books in its library – at least those in the open shelves – and provided in the library the machines by which copies of those books could be made*'. In summary, the copying machines were the 'means' of infringement in the *context* of

the library. Both were essential. His Honour's reasoning and finding proceeded upon the context of both books and copier together and there was no suggestion that the mere provision of a photocopier in the abstract could constitute authorisation: for example (at 13),

> However, in the nature of things it was likely that some of the **books** which were subject to copyright and which **were in the open shelves** might be **copied** by **use of the machines** in a manner that would constitute an infringement of copyright… [emphasis added]

And also at 14:

> The University had the power to control both the use of the **books and** the use of the **machines**. In the circumstances, if a person who was allowed to use the library made a copy of a substantial part of a book **taken from the open shelves of the library**...it can be inferred that the University authorized him to do so… [emphasis added]

There was no suggestion that the university authorised copyright infringement of books brought from home, or outside the library, that happened to be copied on the copiers it had provided. Later decisions have highlighted the importance in *Moorhouse* of both the books and copiers being provided, for example the High Court decision of *Australian Tape Manufacturers Association Ltd and Others v The Commonwealth of Australia* (1993) 177 CLR 480 ('*Australian Tape Manufacturers*') at 498 and *Metro* at [18].

371 The next consideration was knowledge of infringement. Gibbs J found at 14 that the university '*had reasonable grounds to suspect that some infringements would be made if adequate precautions were not taken*' given that it was likely that a copier in a library would be used to copy books which were predominantly copyrighted works, and that it could not be assumed that people would not breach copyright by means of only copying less than a substantial part of a work or by only copying in a manner that constituted fair use for educational purposes. Further, his Honour found (at [14]) that the university was put on notice of the likelihood of infringements by means of a letter from the Australian Copyright Council.

372 As to the third requirement, control, Gibbs J found at 14 that the university '*had the power to control both the use of the books and the use of the machines*'. As mentioned, this statement supports the finding that it was important that both the books *and* the copier were necessary to the finding of authorisation.

373 Gibbs J found therefore at 14 that '*if a person who was allowed to use the library made a copy of a substantial part of a book taken from the open shelves of the library…it can be inferred that the University authorized him to do so, unless the University had taken reasonable steps to prevent an infringing copy of that kind being made*'.

374 Given the previous paragraph, Gibbs J concluded that means, knowledge and control are all that is necessary to constitute a finding of authorisation. Therefore, the role of 'reasonable steps' is to take authorising conduct, or a situation which could be authorising infringement, out of that context, and thereby render what would otherwise be infringing conduct non-infringing. Gibbs J considered (at 15-17) four factors relied upon by the university as reasonable steps to prevent the infringement occurring, namely the provision of a library guide to students with a section dealing with copyright law; the provision of the Copyright Act near the copiers; notices placed on the copiers dealing with the subject of copyright law; and the provision of library attendants. Gibbs J found (at 17) that none of these steps were sufficient to negative the finding of authorisation. They were not '*reasonable or effective precautions against an infringement of copyright by the use of the photocopying machines*'.

375 Consequent upon a finding that there were no reasonable steps taken, and the previous finding that authorisation could be made out in the factual circumstances, his Honour found that the university authorised the copyright infringement of Mr Brennan.

JACOBS J (MCTIERNAN ACJ AGREEING)

376 After referring to similar authority to Gibbs J, Jacobs J found authorisation for slightly different reasons. His Honour began at 21 by stating that authorisation can be found in situations where '*an express permission or invitation is extended to do the act comprised in the copyright or where such a permission or invitation may be implied*'. In the proceedings before him, Jacobs J asked at 21 '*whether there was in the circumstances an invitation to be implied that he [Mr Brennan], in common with other users of the library, might make such use of the photocopying facilities as he saw fit*'.

377 His Honour began by way of creating a hypothetical in which he thought that such implied invitation and thus authorisation could be established, and then compared that hypothetical to the circumstances before him. The hypothetical was:

> …assume first a library open to all persons either freely or on payment of a fee. Assume that the owner places copying machines in the library which can be operated on payment of a fee whereby a profit accrues to the owner of the library. Is this not an invitation to any user to make such use of the machines as he sees fit and therefore an invitation which extends to the doing of acts comprised in the copyright of authors whose books are on the library shelves?...I would certainly answer "Yes"…Authorization is given to use the **copying machine** to **copy library books**. [emphasis added]

The sections in bold provide further evidence of what was discussed at [370] above.

378 Jacobs J then found (at 22) that the mere fact that the library was not open to all was irrelevant and the fact that the university did not make a profit was irrelevant. He found (at 22) the invitation '*extended by the supply of books and machines*' to be an unqualified invitation such that it was not an invitation to only use the copiers to photocopy in a non-infringing way. Therefore, the level of knowledge on the part of the university that infringements were actually occurring was an irrelevancy.

379 His Honour was not persuaded that the library guides, notices or copy of the Copyright Act qualified the invitation he had found. His Honour found at 23, '*Brennan by his conduct accepted the invitation which had no relevant qualification to use the book* "The Americans, Baby" *and the copying machine. The unqualified nature of the invitation sufficiently caused him to do the acts which he did and which were comprised in the copyright of the respondent*'.

380 Relevantly, Jacobs J's finding regarding 'implied invitation' resulted from a critical fact specific to that case, namely the provision of a copier in a library. Copiers have but one use, to copy. However, such supply of copiers is not copyright infringing in the abstract: it is only copyright infringing when applied to a work where such right (copying) is the copyright of the owner of that work. As Jacobs J said at 21, the invitation must be '*extended to do the **act comprised in the copyright***' [emphasis added]. Consequently, the invitation could only be implied because the copier was surrounded by books containing copyright material when

copying was the exclusive right of the copyright owner. The implied invitation was predicated on a copier being placed in a library, not the provision of a copier in the abstract.

CONCLUSION

381 Therefore, whatever reasoning one chooses to consider, both judgments are based upon a fundamental assumption that the alleged authoriser is the one who provided the true 'means' of infringement. The mere provision of facilities by which an infringement can occur will not necessarily constitute infringement. The provision of a photocopier, in the abstract, would not have satisfied the reasoning of either Gibbs or Jacobs JJ. It was the provision of a photocopier *in a library*. The library and provision of books was a distinct and essential ingredient leading to the finding of authorisation.

382 It was only *after* this fundamental and foundational finding that other questions, such as control, power to prevent, knowledge of infringements and so on became relevant. For example, in Jacobs J's reasoning, knowledge is only relevant if there is a qualified, rather than an open, invitation: see 22. However, such consideration is premised upon a finding that there was in fact the implied or express invitation in the first place. Whether or not there is to be an express or implied invitation is to be construed from the factual circumstances. In Gibbs J's reasoning, one has to have under one's control the 'means' of infringement before knowledge of infringement becomes a relevant consideration. Consequently, it is of fundamental importance to decide, in the particular circumstances of each case, whether the person alleged to have authorised actually provided the 'means' of infringement. Context is all important in authorisation proceedings.

Importance of factual context in decisions following Moorhouse

383 While decisions following *Moorhouse* may not explicitly analyse their respective factual circumstances pursuant to the methodology outlined above, it can be discerned from a detailed analysis of those judgments that the findings of authorisation made by them are predicated on a finding that the particular authoriser was the person who provided the 'means' of infringement, and the analysis of considerations relevant to authorisation such as knowledge and power to prevent are predicated upon the initial finding that the 'means' of infringement has been provided by the authoriser.

384 If the decision of *Moorhouse* can be considered the foundation of the contemporary law of authorisation in Australia, the Court considers that the cases since that decision can be divided into two categories: 'technology cases', such as *Australian Tape Manufacturers*, *Cooper* 150 FCR 1, *Cooper* 156 FCR 380, *Kazaa* and the present proceedings; compared with 'APRA cases', such as *Jain* and *Metro*. While both lines of authority follow *Moorhouse* principles, they are factually quite distinct, which should be kept in mind when considering them.

APRA CASES

385 Two key facts are present in the APRA cases. First, the Australasian Performing Right Association Ltd ('APRA') owns the performance rights to the vast majority of music that could or would be performed in public. Second, in each APRA proceeding, the authoriser owned or controlled premises in which live music was performed in public. Consequently, unless those performing at the venue were performing original works which they themselves had created and the performance rights to which had not been assigned to APRA, it would be virtually impossible for the performance rights owned by APRA not to be infringed by the performances at the venue. Consequently, both *Metro* and *Jain*'s factual matrixes were analogous to a copier in a library. Indeed, the context went beyond *Moorhouse*, because it would have been far easier to use a copier in a library in a way that did not infringe copyright, for example, by copying less than a substantial part or for fair use for educational purposes which is an exemption provided by the Copyright Act to infringement, than it would be to use a live music venue in a way that did not infringe APRA's performance rights. As stated in *Metro* at [56]:

> APRA contends that present facts are "relevantly indistinguishable" from those in *Canterbury Bankstown*. This is based on the argument that Metro has power to control what music is performed on its premises, that it **provides facilities for** and advertises **those performances and** that, **whatever songs will be performed, they will be songs in APRA's repertoire**. [emphasis added]

386 In *Jain* the Court appeared to adopt the reasoning of Gibbs J's judgment in *Moorhouse*. The finding of authorisation was predicated upon the foundation that Mr Jain was effectively the CEO of the company that owned a tavern where live music was played and '*the likelihood was that music would be played which would be part of the appellants' repertoire*': see 61. Mr Jain had knowledge of infringements occurring, both general (given

the nature of the live music and APRA's rights) and specific (given a letter from APRA of 12 July 1989 stating that infringements of its copyrights were occurring at the venue): see 61. Mr Jain was found at 61 to have '*the power to control what music was played at the Tavern and also to determine whether a licence from the appellant would be applied for*'. However, he did nothing, taking no reasonable steps to prevent the infringement that was occurring. Consequently, based on the reasoning of Gibbs J, he had authorised the copyright infringements that occurred at the Old Windsor Tavern.

387 No analysis was made by the Full Court in the terms of Jacobs J's 'implied invitation' reasoning. However, one could readily infer from the context of that case, with a live music venue and APRA largely owning the rights to almost any song that was likely to be played there, that the provision of the premises to those playing live music was a relevantly unqualified invitation to use the venue to infringe APRA's copyright, remembering that the invitation must be one '*extended to do the act comprised in the copyright*': see [376] above.

388 In *Metro* it was argued (at [15]) that there was a contractual arrangement between the premises and the promoter whereby the promoter was to gain the relevant APRA licence, which would, in Jacobs J's reasoning, qualify the invitation. However, it was also found in that case that the promoters had not obtained the licences and Metro knew this. Therefore, the invitation in that decision was relevantly unqualified and *Metro* thereby authorised the infringement that resulted.

TECHNOLOGY CASES

389 The 'technology' decisions display the requirement for the authoriser to have provided the 'means' of infringement even more clearly. Although the High Court decision of *Australian Tape Manufacturers* involved a dispute regarding constitutional law, a necessary step in the reasoning of the decision was to consider whether a vendor who sold blank tape and/or tape recorders would authorise any infringement that resulted from the use of those items. The High Court found (at 498) that:

> [i]t follows that manufacture and sale of articles such as blank tapes or video recorders, which have lawful uses, do not constitute authorization of infringement of copyright, even if the manufacturer or vendor knows that there is a likelihood that the articles will be used for an infringing purpose such as home taping of sound recordings, so long as the manufacturer or vendor has no control over the purchaser's use of that article.

390 The High Court drew a distinction (at 498) between the facts in those proceedings and those in *Moorhouse* where the university had control and had '*provided potential infringers with both the copyright material and the use of the University's machines by which copies of it could be made*'. It would appear that the High Court preferred the analysis of Gibbs J to that of Jacobs J, because there was no analysis whether the sale of blank video tape or recorders could constitute an unqualified invitation to use that tape to infringe copyright, thus authorising the copyright infringement which resulted from its use. It would appear under Jacobs J's analysis of authorisation that control at the time of the infringement itself was not an essential element in the circumstance that an invitation can be implied from the mere sale of goods. While it is always dangerous to attempt to explain why something was not said or considered in a judgment, it is at least arguable that given their Honour's explicit approval of comments made in *CBS Songs Ltd and Others v Amstrad Consumer Electronics PLC and Another* [1988] AC 1013 ('Amstrad') and *Sony Corporation of America v Universal City Studios Inc* 464 US 417 (1984) (to the effect that while tape recorders facilitated infringement they were '*capable of non-infringing uses*') that the tape's sale of itself could not constitute an implied invitation to do a copyright act. In that sense the tape or recorder would be a copier in the abstract. In both Amstrad and Sony there was no liability even thought there was evidence that such machines could be used, and were used, for copyright infringement.

391 Such assessment of tape and recording devices can be contrasted with the facts in *Cooper* 150 FCR 1. In that decision, the fundamental basis of Tamberlin J's finding that Mr Cooper authorised infringement was the following factual finding (at [84]):

> The Cooper website is carefully structured and highly organised. Many of its pages contain numerous references to linking and downloading. The website also provides the hyperlinks that enable the user to directly access and download the files from the remote websites. **The website is clearly designed to – and does – facilitate and enable this infringing downloading.** I am of the view that there is a reasonable inference available that Cooper, who sought advice as to the establishment and operation of his website, knowingly permitted or approved the use of his website in this manner and **designed and organised it to achieve this result**. [emphasis added]

392 Critically, based upon Gibbs J's reasoning, Mr Cooper's website was clearly the 'means' of infringement. On Jacobs J's reasoning it was an express invitation to users to use the website to infringe copyright. The facts in *Cooper* 150 FCR 1 in fact went well beyond that in *Moorhouse* in that Tamberlin J found that Mr Cooper *intended* that the website be

used to infringe copyright. There is no suggestion in *Moorhouse* that the university intended its copiers and books be used to infringe copyright.

393 It was only after making such funding that Tamberlin J went on (at [85]-[87]) to analyse whether Mr Cooper had the requisite control over the 'means' of infringement as per Gibbs J; whether the disclaimers on Mr Cooper's website regarding copyright were a reasonable step to prevent infringement as per Gibbs J; and finally to find that Mr Cooper did not take a reasonable step, namely to remove the hyperlinks that linked to infringing music files.

394 The role played by Comcen, the ISP which also was found to have authorised infringement, will be considered below. On appeal in *Cooper* 156 FCR 380, Branson J found similarly to Tamberlin J at [41] regarding the actions of Mr Cooper:

> I conclude that, within the meaning of the paragraph [s 101(1A)(a)] a person's power to prevent the doing of an act comprised in the copyright includes the person's power not to facilitate the doing of that act by, for example, making available to the public a technical capacity **calculated to lead to the doing of that act**. [emphasis added]

That added proviso, that Mr Cooper did not just provide the facilities in the abstract, rather he provided them in a *calculated* way to bring about the infringements that resulted, is to be noted. It may have been inferred that Mr Cooper so calculated due to his design of the website, the name of the website, as well as the fact that, as was conceded on appeal at [2], the '*overwhelming majority*' of links on Mr Cooper's website linked to infringing material. This would satisfy Jacob J's 'implied invitation' analysis as well as Gibbs J's provision of the 'means' of infringement approach. Indeed, Branson J, in analysing *Moorhouse*, said at [36]:

> It seems to me that both Jacobs and Gibbs JJ concentrated on the behaviour of the University in making the photocopier available for use in the library rather than on the issue of the University's capacity to control the use of the photocopier once it had been made available to library users…That is, the relevant power which the University had to prevent the copyright infringement must be understood to have been, or at least to have included, the power not to allow a coin-operated photocopier in the library.

395 At [149] Kenny J explicitly relied on the finding extracted in the paragraph above at [391] to make the following finding:

> [t]he findings at first instance as to the nature, the contents and structure of the website, which were not seriously contested, plainly supported the further finding

> that Mr Cooper **deliberately designed the website to facilitate infringing downloading of sound recordings**. Mr Cooper's position was, in this respect, entirely different from that of the manufacturers and vendors of blank tapes, which was considered in *Australian Tape Manufacturers* 176 CLR 480. [emphasis added]

396 Later, adopting (though not explicitly) the reasoning of Jacobs J, Kenny J said at [152]:

> So far as internet users and remote website operators were concerned, the website was in substance an invitation to use the hyperlinks provided and to add new links in order that sound recordings could be downloaded from remote websites, and a principle purpose of the website was to enable infringing copies of the downloaded sound recordings to be made. The fact that the website also carried a warning that some downloading could be illegal did not lessen the force of the invitation.

Kenny J found that the provision of Mr Cooper's website was an implicit or explicit unqualified invitation to use his website to infringe.

397 In *Kazaa*, similar considerations applied. The Kazaa system's predominant use, and perception of its use by its users, was as a tool for copyright infringement and this was known to its creators. Wilcox J specifically found at [194] that it was the intention of its creators to have the Kazaa system used for copyright infringement, '*[n]one of them had an interest to prevent or curtail that predominant use [copyright infringement]; if anything, the contrary*': that is, it was their intention to invite infringement. A summary of the evidence supporting that proposition is found at [181]-[193] of his Honour's judgment. It included a focus group report commissioned by Sharman stating that Kazaa was perceived and used by its users primarily for copyright infringement of music; emails between Sharman executives regarding how to promote file-sharing; and the advertising of the Kazaa system itself, particularly the '*Join the Revolution campaign*' which constituted positive encouragement to use the Kazaa system to infringe. In accordance with the reasoning of Gibbs J, this was the provision of the 'means' of infringement. Consistent with Jacobs J, this could be seen as an explicit invitation to use the facilities to infringe.

398 Returning to the position of Comcen vis-à-vis authorisation, the Court considers that while the ISP did not provide the 'means' of infringement in the same sense that Mr Cooper did, given that Comcen not only helped set up the website but also made contractual arrangements with Mr Cooper for the hosting of his website free of charge, Comcen must be seen, in light of Tamberlin J's reasons, to have been so complicit in the existence of the website (which was the 'means' of infringement) that it provided such facility in the same

way that Mr Cooper himself did. Indeed, Tamberlin J pointed out at [131] the fact that Comcen had:

> …assumed an active role by agreeing to host the website and assisting with the operation of the website…[t]he reciprocal consideration passing between them, namely, the free hosting in return for the display of the Com-cen logo on the website is an additional matter…

399 Consequently, while the liability of Comcen for copyright infringement in *Cooper* suggests that it is possible for an ISP to authorise infringement, it is important to observe the very specific factual circumstances in which authorisation was found. Comcen had directly dealt with, and assisted in the creation of, the particular 'means' of infringement (the website), and had even entered into an agreement with its owner to provide for hosting of that website free of charge.

Did the respondent provide the 'means' of infringement?

400 It is important to distinguish between the provision of a necessary precondition to infringements occurring, and the provision of the actual 'means' of infringement in the reasoning of Gibbs J in *Moorhouse*. As discussed earlier, a photocopier can be used to infringe copyright, but on the reasoning of Gibbs J and Jacobs J, the mere provision of a photocopier was not the 'means' of infringement in the abstract. Rather, it was only the 'means' of infringement in the particular context of the library, where it was surrounded by copyright works. Other preconditions existed, namely the supply of power and the physical premises in which the infringements occurred. The presence of each of these factors was a necessary precondition for the infringements to occur, but that does not inexorably lead to the conclusion that a person who individually provided each one of those preconditions could equally be found to have authorised the infringements.

401 In the present circumstances, it is obvious that the respondent's provision of the internet was *a* necessary precondition for the infringements which occurred. However, that does not mean that the provision of the internet was *the* 'means' of infringement. The provision of the internet was just as necessary a precondition to the infringements which occurred in the *Kazaa* proceedings, but no ISP was joined as a respondent. The focus in that proceeding was correctly upon the more immediate means by which the infringements occurred, namely the Kazaa system. Indeed, the applicants' closing submissions in reply

regarding the centrality of the provision of the internet (rather than the BitTorrent system) to infringing the communication right would suggest that *Kazaa* was wrongly decided and therefore the Court rejects them. The provision of the internet was also a necessary precondition to the infringements that occurred by the people who accessed Mr Cooper's website, but, again, the focus in those proceedings was rightly upon the narrower and more specific 'means' of infringement, namely the website and the ISP that hosted it. As with cases like *Kazaa* and *Cooper*, in the present circumstances there are also other necessary preconditions to bring about infringement, such as the computers upon which the infringements occurred or the operating systems on those computers, for example, Microsoft Windows.

402 The use of the BitTorrent system as a whole was not just a precondition to infringement; it was, in a very real sense, the 'means' by which the applicants' copyright has been infringed. This is the inevitable conclusion one must reach when there is not a scintilla of evidence of infringement occurring other than by the use of the BitTorrent system. Such conclusion is reinforced by the critical fact that there does not appear to be any way to infringe the applicants' copyright from mere use of the internet. There will always have to be an additional tool employed, whether that be a website linking to copyright infringing content like Mr Cooper's website in *Cooper*, or a p2p system like the Kazaa system in *Kazaa* and the BitTorrent system in the current proceedings. Absent the BitTorrent system, the infringements could not have occurred.

403 The infringing iiNet users must seek out a BitTorrent client and must seek out .torrent files related to infringing material themselves. In doing so, they are provided with no assistance from the respondent. The respondent cannot monitor them doing so or prevent them from doing so.

404 For the abovementioned reasons, the Court finds that it is not the respondent, but rather it is the use of the BitTorrent system as a whole which is the 'means' by which the applicants' copyright has been infringed. The respondent's internet service, by itself, did not result in copyright infringement. It is correct that, absent such service, the infringements could not have taken place. But it is equally true that more was required to effect the infringements, being the BitTorrent system over which the respondent had no control.

405 All the evidence of the infringement of the applicants' films before the Court was generated by means of the use of the BitTorrent system. The DtecNet Agent operates as a BitTorrent client and participates in swarms. Mr Herps and Mr Fraser downloaded a BitTorrent client onto their computer and participated in BitTorrent swarms in order to infringe the applicants' copyright. All the particularised acts of infringement pleaded by the applicants in the applicants' particulars derive from the BitTorrent system. As the applicants said in their closing submissions, '*[i]nsofar as the applicants allege that iiNet users have engaged in acts of infringement in the course of accessing the internet by means of iiNet's internet services, those users have done so using the BitTorrent protocol*'.

406 In making such finding the Court does not wish to imply that the BitTorrent system is necessarily copyright infringing, nor that the BitTorrent system itself is illegal. Rather, that in the particular circumstances of these proceedings it is the 'means' of infringement, it having been deliberately used by persons to achieve this consequence. The Court expressly declines to find whether any constituent part of the BitTorrent system is the precise 'means' of infringement. As stated at [70]-[72], the BitTorrent system cannot sensibly be seen as anything other than all the constituent parts of that system working together.

407 There is no evidence before this Court that the respondent has any connection whatsoever with any part of the BitTorrent system. The respondent has no dealings with any organisation which produces BitTorrent clients. The respondent has no dealings with any website that makes available .torrent files that relate to infringing material. The respondent does not support any software, let alone software that is a constituent part of the BitTorrent system. Merely directing those asking questions about BitTorrent to a location where they can gain more information does not constitute 'support'. The respondent did make available a press release in relation to this proceeding via the BitTorrent system, but there is nothing untoward in using this system and it is not evidence of any relationship between the respondent and any of the constituent parts of the BitTorrent system.

408 In this sense the respondent is in an entirely different position to Comcen in *Cooper*, and this critical factual distinction is pivotal. In that proceeding, not only did the ISP host the 'means' of infringement (Mr Cooper's website) on their servers, they actively supported Mr Cooper in the creation of that website, and even entered into a contractual arrangement with

him whereby Mr Cooper's website was hosted free of charge in exchange for Mr Cooper advertising Comcen on his website by means of a logo and link to Comcen's website.

409 In fact it was found at [157] of *Cooper* 156 FCR 380 by Kenny J that '*E-talk could have taken down the website itself. It could have declined to provide its host facilities*'. Branson J said at [64] that Comcen could have withdrawn the hosting of the website or otherwise placed pressure on Mr Cooper '*to stop his website being used for the predominant purpose of copyright infringements*'. In the present proceeding the respondent has no ability to do anything in relation to the BitTorrent system. It cannot pressure, cajole or threaten any BitTorrent client, or shut down any website hosting .torrent files associated with copyright infringing material. It could terminate the accounts of iiNet users who infringe but that is termination of the provision of the internet which, while certainly a precondition to the infringements, is not the 'means' by which those infringements occur.

410 The internet can be used to virtually any end. Mr Malone cited examples including communication, such as email, social networking websites and VOIP; online banking and retailing; and entertainment, such as through online media and games. The Court takes judicial notice of the fact that the internet is increasingly the means by which the news is disseminated and created.

411 While the Court expressly does not characterise access to the internet as akin to a 'human right' as the Constitutional Council of France has recently, one does not need to consider access to the internet to be a 'human right' to appreciate its central role in almost all aspects of modern life, and, consequently, to appreciate that its mere provision could not possibly justify a finding that it was the 'means' of copyright infringement. This position may be contrasted with the *Kazaa* system which was found to be predominantly used for, and certainly seen by its users as, the 'means' to infringe copyright. Similarly, the overwhelming majority of hyperlinks on Mr Cooper's website went to copyright infringing material.

412 Indeed, it is this very broadness of the uses of the internet which provides a clear distinguishing factor to other cases where authorisation was found. In the APRA cases, as already explained, there was very little use to which a live music venue could be put other than infringing copyright in the circumstances that APRA owned the performance rights of virtually every song that would be performed at such a venue and no licence was obtained.

On the facts in both *Metro* and *Jain* there did not appear to be any relevant use of the venue for a non-infringing purpose, such as artists performing their original works for which APRA did not hold the performance rights. In *Kazaa*, as mentioned, the predominant use of the Kazaa system was to infringe. The overwhelming use of Mr Cooper's website was to infringe. In *Australian Tape Manufacturers* the High Court explicitly mentioned that tape and video recorders '*have lawful uses*', suggesting that it was at least part of the reason why authorisation was not made out. The Court would note that the lawful uses of video recorders and tape were then far fewer than the internet has today. Indeed in *Amstrad*, which was relied upon in *Australian Tape Manufacturers*, Lord Templeman stated at 1050 that, '*[i]t is statistically certain that most but not all consoles are used for the purpose of home copying in breach of copyright*' (yet the authorisation of infringement was not found).

413 It is this broadness of the various uses of the internet which explains why its mere provision is not an implicit invitation in the sense discussed by Jacobs J in *Moorhouse*. The relevant invitation was one (at 21) which was '*an invitation to any user to make such use of the machines as he sees fit and therefore an invitation which extends to the doing of acts comprised in the copyright of the authors whose books are on the library shelves*'. It was, as mentioned, an invitation '*extended to do the act comprised in the copyright*'. However, the mere use of the internet cannot infringe copyright without more. The provision of the internet is not an implicit invitation to use it to infringe copyright, even if it is an unqualified invitation. The Court cannot imply such invitation in the present circumstances. Perhaps if the predominant use of the internet was to infringe copyright, its provision might constitute such an invitation. Perhaps if there was an additional relevant contextual factor, such as the existence of the library context in *Moorhouse*, an invitation to infringe could be implied. But in the circumstances of this case, the Court simply cannot find such implicit invitation to infringe as Jacobs J could in *Moorhouse*. On the facts before his Honour, there were copiers, whose one use was to copy, in an environment saturated with copyright works where one of the copyrights in those works was the exclusive right to copy. The internet has a litany of uses, and it is not saturated with copyright works in the same sense.

414 In conclusion, the Court considers that the respondent did not provide the 'means' of infringement in the sense that the phrase was used by Gibbs J. It did not extend an invitation to the iiNet users to use its facilities to do acts comprised in the copyright of the applicants.

Consequently, the Court finds that the respondent did not authorise the infringement of copyright carried out by the iiNet users.

Section 101(1A) considerations

415 Wilcox J at [402] in *Kazaa* made clear that, citing Bennett J in *Metro*, s 101(1A) was meant to elucidate, not vary, the pre-existing law of authorisation. This conclusion was approved by Branson J at [20] and Kenny J at [136] in *Cooper* 156 FCR 380. Consequently, the discussion above continues to guide the Court to its conclusion that the respondent did not authorise the infringement of the iiNet users. Therefore, the Court would find that the respondent did not authorise for the reasons discussed above regardless of its consideration of s 101(1A) of the Copyright Act below.

416 Nevertheless, as s 101(1A) is phrased as considerations that '*must*' be considered, the Court is compelled to go into further consideration of the issue of authorisation pursuant to the considerations in s 101(1A)(a)-(c) of the Copyright Act.

Section 101(1A)(a) Power to prevent

417 Section 101(1A)(a) provides the first statutory consideration, specifically '*the extent, (if any) of the person's power to prevent the doing of the act concerned*'. The Court considers that a power to prevent is not an absolute power to prevent. As already discussed, there is a distinction between a precondition to infringement and the 'means' of infringement. Any number of persons may have control over whether a precondition exists, and therefore have the power to prevent the infringement by refusing to provide the precondition, but the Court does not believe that all such persons have the power to prevent the infringement relevant to a finding of authorisation and s 101(1A)(a).

AUTHORITY

418 The term 'control' which appears in the test of Gibbs J in *Moorhouse* (extracted at [369] above), and 'power to prevent' appear to be treated synonymously in the authorities: see, for example, Gibbs J's reference in *Moorhouse* at 12 to two different statements in *Adelaide Corporation* (one using the term 'control', the other 'power to prevent') in support of the same proposition; see also *Metro* at [67]; and *Kazaa* at [414]. Control (and therefore

the power to prevent) is, pursuant to *Adelaide Corporation* at 497-498 and 503 and *Moorhouse* at 12, essential to a finding of authorisation. Such statement has never been adequately reconciled with Jacobs J's 'implied invitation' reasoning which would appear to envisage authorisation where there was no control, aside from the initial offer of the 'means' to infringe: see, for example, the Court's discussion of *Australian Tape Manufacturers* at [390] above. Regardless, Gibbs J's determination on this point has never been questioned and it is accepted by both parties in these proceedings that control must necessarily be found to exist before there can be a finding of authorisation.

419 However, this control and power to prevent does not extend indefinitely. The clearest example of this is the decision of *Australian Tape Manufacturers*. In that decision, as discussed, the High Court considered that the vendor had no relevant control over the use of the tape or tape recorders following their sale. However, the vendor always had the ability to not offer the products for sale at all. Similarly, the manufacturer could have never created the items in question. That must have been a relevant consideration to their ability to 'control' infringement. It was determined to be relevant for the purposes of the 'power to prevent' discussion at [36]-[37] and [41] of Branson J's decision in *Cooper* 156 FCR 380 where her Honour said at [41]:

> I conclude that, within the meaning of the paragraph, a person's power to prevent the doing of an act comprised in a copyright includes a person's power not to facilitate the doing of that act by, for example, making available to the public a technical capacity calculated to lead to the doing of that act.

The only way to reconcile Branson J's statement with *Australian Tape Manufacturers* where authorisation was found not to exist (assuming her Honour did not desire to depart from existing High Court authority) is to conclude that in *Australian Tape Manufacturers* the sale of tape and video recorders was not *calculated* to lead to the infringement of copyright. Tape and recording equipment certainly has a '*technical capacity*' to infringe copyright and it was '*made available to the public*'. It was this '*calculation*' aspect which Kenny J used (at [149]) to distinguish *Australian Tape Manufacturers* from the situation before her in *Cooper* 156 FCR 380. It is a fine distinction, given that in *Amstrad*, as already discussed, it was found to be '*statistically certain that most…consoles are used*' for copyright infringing purposes and the High Court did not suggest otherwise in *Australian Tape Manufacturers*, observing that there were '*lawful uses*' for tape, not necessarily that tape would be used lawfully. There is also discussion of the issue in *Hanimex* at 286-287. These passages provide clear guidance

that the power to prevent infringement or exercise control over infringement is not an absolute, and whether the alleged authoriser has the relevant control or power to prevent the infringements will be determined by the factual matrix present in each case.

420 In *Adelaide Corporation*, Higgins J at 498-499 considered that while it was possible to prevent copyright infringement by means of cancelling a lease with persons using a hall who were performing copyright works without licence, cancelling the lease was '*not a step which would in itself prevent the infringement of the copyright, but a step which would do much more: it would put an end to the lease*'. It cannot be doubted that such statement was made in the context of a consideration of 'permission' rather than 'authorisation' but, as already explained at [369] above, *Moorhouse* made clear that the two words were treated synonymously in *Adelaide Corporation*. This is further indicia that a power to prevent is not to be interpreted as an absolute power to prevent.

421 Explicit in Higgins J's consideration in *Adelaide Corporation* was that notions of reasonableness of steps which might be taken and the power to prevent infringement interact: '*[i]s the smashing of the lease a "reasonable step" under the circumstances?*' (at 499). Therefore, it appears that there is necessarily interaction between s 101(1A)(a) and (c) of the Copyright Act in that one could not be said to have the power to prevent infringement if the step to be taken to prevent the infringement is not a reasonable step in the circumstances. For example, the factors that led Kenny J at [155] to find that Comcen had the power to prevent the infringements occurring by Mr Cooper's website were the same factors her Honour mentioned at [157] in relation to reasonable steps that could have been taken (but were not) by Comcen. The same can be said of Branson J's reasoning at [62] and [64].

422 Finally, it should be noted from the reasoning of authorisation decisions themselves that judges have been keen to closely confine a finding that there is a power to prevent or control infringement to steps that would be reasonable and proportionate in the circumstances. For example, in *Kazaa*, Wilcox J at [411] expressly conditioned his finding that the respondents in those proceedings had the relevant power to prevent infringement on his specific findings in regards to the narrow technical mechanisms that could be employed to curtail infringement on the Kazaa system: '*[i]f I am correct in my conclusions about keyword filtering…and gold file filtering…Sharman had power (in the case of gold file flood filtering,*

in conjunction with Altnet) to prevent, or at least substantially to reduce, the incidence of copyright file-sharing'. His Honour did not find that the power to prevent extended to shutting down the Kazaa system as a whole, even though such act would, in an absolute sense, prevent the infringement that was occurring. In *Moorhouse* Gibbs J at 15 mentioned that a reasonable step might have been to include a '*clearly worded and accurate notice on each machine in a position where it could not be overlooked*', being a power to prevent infringement of a lower standard than not offering the photocopiers in the library which would, in an absolute sense, be a power to prevent infringement (though in *Cooper* 156 FCR 380 at [36] Branson J thought otherwise). Mr Cooper had his website shut down completely, depriving him of income, but this was necessary in the context where it was found that he provided facilities calculated to lead to infringements; the overwhelming majority of the use of his site was to infringe; and that he intended that to be so.

423 As Kenny J said in *Cooper* 156 FCR 380 at [142], '*[t]he question what degree of control can constitute a sufficient basis for a finding of authorisation does not admit of a straightforward answer*': see also *Hanimex* at 286-287.

DID THE RESPONDENT HAVE THE POWER TO PREVENT THE INFRINGEMENTS?

424 In the present circumstances, it must be remembered that the Court has found that the respondent has not provided the 'means' of infringement. It has provided one of the facilities which has enabled infringements to occur, but that is a distinct consideration: see [400]-[414] above. The BitTorrent system is the 'means' of infringement. As already outlined, the respondent had no relevant power over any aspect of the BitTorrent system: see [407]-[409] above. Consequently, the Court finds that the only relevant power the respondent had to prevent infringement was to warn and then terminate/suspend its subscriber's accounts based on the AFACT Notices. Other technical mechanisms were mentioned from time to time in the proceedings, such as play-penning (restricting accounts), and, at one point, blocking websites. However, there was inadequate evidence before the Court to make any finding regarding the scope and effectiveness of such mechanisms. This may be contrasted with *Kazaa* where it is evident from Wilcox J's decision at [254]-[294] and [310]-[330] that there was extensive evidence before the Court of the feasibility of the technical mechanisms that his Honour eventually found would prevent or substantially curtail infringement, namely '*keyword filtering*' and the '*gold file flood*'. This issue is discussed further at [459] below.

APPLICANTS' SUBMISSIONS THAT THE RESPONDENT DID HAVE THE POWER TO PREVENT INFRINGEMENTS

425 The applicants make four primary submissions why the respondent had the relevant power to prevent the infringements which were occurring by means of warning and suspension or termination of the iiNet users. First, the respondent's ability to do so under the CRA; secondly, the fact the respondent does so in other circumstances; thirdly, the safe harbour provisions; and fourthly, the technical capability of the respondent to suspend and cancel accounts.

426 There can be no doubt that the respondent has the contractual right to warn and terminate its subscribers pursuant to its CRA if a breach of its terms occurs. However, that does not, of itself, make termination a reasonable step or a relevant power to prevent infringement in all circumstances. It must be remembered that absent those contractual provisions, the respondent would have had no power to terminate subscribers even if they were found by a Court to have infringed copyright. The CRA constitutes the respondent's standard contractual terms used by a wide variety of subscribers. Consequently, and unsurprisingly, the CRA seeks to provide sufficient contractual terms to cover all eventualities, both existing at the time of the writing of the CRA and into the future. That does not mean that such terms should or would always be exercised even if a contractual right to exercise them arises.

427 Further, the right to do something does not create an obligation to do something. The doctrine of privity of contract provides that the only two parties relevant to the enforcement of the CRA are the respondent and the subscriber. Should the contract be breached by the subscriber, it is entirely a matter for the respondent to decide whether to act on the contract. Had the respondent taken action against its subscribers based on an AFACT Notice and it was subsequently found that the allegation was unfounded, the respondent would have committed a breach of its contract with the subscriber and been made potentially liable for damages without any indemnity from the applicants or AFACT. In such circumstance it was not unreasonable that the respondent should have sought to be cautious before acting on information provided by a party unrelated to the CRA.

428 As Bennett J in *Metro* said at [61] '*[t]he extent to which a party is obliged to use legal powers in a contract in order to take reasonable steps must, I would have thought, vary with the facts of the particular case*'. If the respondent did not have the power to terminate subscribers' accounts, that may well have been a relevant factor suggesting it did not have a power to prevent infringements, but it does not follow that the corollary applies with equal force.

429 As to the applicants' second submission, it is clear that the respondent, from time to time, suspends or terminates subscriber's accounts on the basis of non-payment of fees, that is, for non-compliance with contractual obligations. The applicants question why it is reasonable to terminate in these circumstances and not on the basis of the AFACT Notices. The reason is simple. The respondent could take action following the non-payment of fees because there is a far greater degree of certainty whether an account is financial or otherwise. The enquiry is straightforward. The respondent has all the information before it necessary to make a decision as to whether that contractual obligation has been complied with by its subscribers. The evidence of Mr Dalby demonstrated that even though the non-payment of fees might be obvious, the respondent exercised significant discretion when exercising the power to suspend or terminate an account. Further, even though failure to pay fees is an uncomplicated issue, the respondent's right to terminate operates in the context of the Telecommunications Ombudsman being expressly charged with oversight to deal with complaints regarding billing: see s 128(5) *Telecommunications (Consumer Protection and Service Standards) Act*.

430 The same cannot be said of copyright infringement. Regardless of the actual quality of the evidence gathering of DtecNet, copyright infringement is not a straight 'yes' or 'no' question. The Court has had to examine a very significant quantity of technical and legal detail over dozens of pages in this judgment in order to determine whether iiNet users, and how often iiNet users, infringe copyright by use of the BitTorrent system. The respondent had no such guidance before these proceedings came to be heard. The respondent apparently did not properly understand how the evidence of infringements underlying the AFACT Notices was gathered. The respondent was understandably reluctant to allege copyright infringement and terminate based on that allegation. However, the reasonableness of terminating subscribers on the basis of non-payment of fees does not dictate that warning and termination

on the basis of AFACT Notices was equally reasonable. Unlike an allegation of copyright infringement, the respondent did not need a third party to provide evidence that its subscribers had not paid their fees before taking action to terminate an account for such reason.

431 As to the applicants' third submission, the applicants submit that as condition 1 of item 1 of s 116AH(1) of the Copyright Act expressly envisages termination of subscriber accounts, such step is, by force of statute, necessarily a reasonable step and is therefore a relevant power to prevent infringement. Such submission is not only circular; it is misconceived in its understanding of the safe harbour provisions found in Division 2AA of Part V of the Copyright Act. Such provisions are discussed in detail later in the judgment in Part F. Suffice to say, as the Court will explain, failure to comply with the safe harbour provisions is not a factor which can be used for the purposes of supporting a finding of authorisation, given that they are optional.

432 Even if the Court be wrong in making such finding, the applicants' reasoning is circular. Condition 1 of item 1 of s 116AH(1) is phrased as '*a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers*'. '*[A]ppropriate circumstances*' is not defined. Termination may be reasonable in '*appropriate circumstances*'. However, given that no guidance is given by the legislature as to what those '*appropriate circumstances*' might be, it cannot be said that the mere existence of the provision renders termination reasonable. It only renders it reasonable in '*appropriate circumstances*'. If '*appropriate circumstances*' are found to exist only when a Court finds someone to have infringed copyright, then the respondent's termination of an account for a reason which did not satisfy that requirement would expressly not be reasonable, on the applicants' own reasoning.

433 Finally, the applicants argue that the respondent has the technical capability to suspend and terminate accounts. The Court accepts that this is the case. However, the technical feasibility of suspension and termination is not the only relevant consideration. It must be noted that such technical capacity does not operate in a vacuum: it must be considered in the context of the reasons for which it would be exercised. The applicants point to the Westnet policy as evidence of the feasibility of such a scheme of warning and

termination. However, the evidence demonstrates that Westnet's policy was to pass on warning notices received by it to its subscribers, and to do no more. It may be readily assumed that merely passing on notices could hardly be a power to prevent infringement or a reasonable step without more, given that a person intent on infringing would quickly become aware that such warnings were ineffectual if termination of accounts did not follow, similarly to the position of notifications not to infringe copyright in *Kazaa* (for example, at [407]). That is, an ineffectual step is not a power to prevent infringement nor is it a reasonable step. As extracted at [138] above, '*no further action (beyond forwarding the notices) is taken*'. That can hardly be a power to prevent infringement. Therefore, all the applicants' submissions suggesting that it would be a simple and reasonable step to implement a scheme for passing on warning notices has no merit.

434 Even assuming that Mr Malone's evidence relating to the feasibility of a notification/warning system referred to in his second affidavit were wrong and that such system could be implemented with ease, the primary feasibility problem remains. The primary problem arises from the considerations identified in Mr Malone's second affidavit at [17] regarding the difficulty in imposing a notification *as well as* a disconnection regime. It is by no means clear how many infringements ought to lead to termination; whether a sufficient number can happen within one notification, or whether time should be given for behaviour to be rectified; whether termination should only occur in relation to infringements made on the basis of evidence generated by a DtecNet-style process or whether notices such as those sent by the US robot notices also ought to result in termination; and how to deal with subscribers disputing the accuracy of notifications of infringement. Indeed, the applicants also mention 'suspension' of accounts as an option, that is, a step short of termination. This would appear to be a suggestion that subscribers could be sanctioned by suspending internet access for a period. However, the duration required for any proposed suspension is unknown and it is unclear whether, for example, it ought apply only to iiNet users whose infringement were on a small scale. The respondent had no certainty, even if it took some steps, whether it might nevertheless be taken to have authorised infringement. As the Court has just found, had the respondent been sued, merely passing on notifications as Westnet did would not have been sufficient in itself for the Court to conclude that the respondent had taken a reasonable step to prevent the infringement of copyright and thus did not authorise.

435 One need only consider the lengthy, complex and necessary deliberations of the Court upon the question of primary infringement to appreciate that the nature of copyright infringements within the BitTorrent system, and the concept of 'repeat infringer', are not self-evident. It is highly problematic to conclude that such issues ought to be decided by a party, such as the respondent, rather than a court. Copyright infringement is not a simple issue. Such problems as identified are not insurmountable, but they do weigh against a finding that the respondent could conclusively decide that infringement had occurred and that it had the relevant power to prevent by warning, suspension or termination of subscriber accounts, even if it had the technical capability to do so. Even if feasible, such a scheme would likely lead to significant expense incurred by the respondent, as was alluded to by Mr Malone in his second affidavit. Of course significant expense was likely to have been incurred by the respondents in *Kazaa*, but that was in the context of those respondents having provided the 'means' of infringement. The respondent has not done so in these proceedings, and thus the expense and complexity of the imposition of responsibility for a notice and termination scheme on them manifestly militates against the conclusion that such scheme is a relevant power to prevent.

THE COURT'S CONSIDERATION

436 The Court does not consider that warning and termination of subscriber accounts on the basis of AFACT Notices is a reasonable step, and further, that it would constitute a relevant power to prevent the infringements occurring. The respondent did not create the 'means' to infringe copyright. It was the constituent parts of the BitTorrent system which has given rise to the infringements. Consequently, it cannot be incumbent upon the respondent to stop the infringements. Even if it was incumbent upon the respondent, that does not lead to the conclusion that it was a reasonable step for it to take action. Termination of internet facilities might have been reasonable in *Cooper*, but that was a decision regarding the hosting of a website which was calculated to, and was overwhelmingly used to, infringe with the creation of such website being actively assisted by the ISP, Comcen.

437 Even taking the RC-20 accounts where infringements have been shown to have occurred, it is not at all clear whether those accounts were used primarily, substantially or even significantly for the infringement of the applicants' copyright. Schedule 1 of the respondent's closing submissions provides some indication that at least in the accounts where significant evidence is before the Court, and where significant repeat infringements have

been proven, copyright infringement is not a primary or even significant usage of quota on those accounts. That is, even on what would appear to be some of the worst examples of infringing iiNet users and assuming (against the Court's earlier finding) that the provision of the internet is the 'means' of infringement, the infringement of the applicants' copyright does not even appear to be a significant use of quota on those accounts. This should be contrasted with Mr Cooper's website and the Kazaa system.

438 Obviously termination of the subscriber accounts would constitute a step that would prevent the person or persons from infringing (at least with that ISP), but it would also prevent that person or persons from using the internet for all the non-infringing uses to which the internet may be put and to which they have contracted with the respondent and provided consideration. Given that Wilcox J had no desire to order the respondents in *Kazaa* to shut down their system where he found the *predominant* use was to infringe copyright, it would seem that termination of accounts in the circumstances of unproven and sporadic use, at least absent judicial consideration of the extent of the infringement on each account, would be unreasonable. The words of Higgins J in *Adelaide Corporation* are apposite. While termination of accounts would stop the infringement, it would do much more and in the circumstances it would not be reasonable. Consequently, warning and termination/suspension does not relevantly constitute a power to prevent infringement on the part of the respondent.

439 There is a distinction to be observed between what the applicants seek and that which was sought in previous authorisation proceedings considered earlier in this judgment. In no previous proceeding has any attempt been made to render an alleged authoriser responsible for, or to act as, a conduit to punish those who are responsible for infringing the applicants' copyright directly. In a substantive sense, the applicants seek an extrajudicial scheme for the imposition of collective punishment for those alleged to have committed a tort (that is, the iiNet users). It inevitably follows from this argument that those that fail to participate in such scheme (that is, the respondent) themselves also commit a tort.

440 Presuming that the MPA and AFACT can speak for the applicants (which one assumes must be the case, otherwise these proceedings would never have been instituted) the applicants have made clear their desire to sanction via the respondent those directly infringing copyright, that is, the iiNet users. A letter dated 25 June 2008 by Mr Pisano, the

President of the MPA, to Mr Coroneos, the CEO of the IIA, stated '*[o]ur view is that some adequate sanction is necessary in the implementation of a graduated response program in order for it to be effective to both educate the user and discourage repeat infringements*'. Mr Gane said that the '*graduated program*' proposed by AFACT in a press release dated 29 August 2007 (exhibit 3) '*would have encapsulated a series of sanctions that an ISP could have taken*' (despite the press release stating that '*[t]he graduated response AFACT is proposing isn't about punishing customers – it's about educating customers*'). Such punishment or sanction would be collective because the termination or suspension of a subscriber account would affect not just the person who infringed, but all those who access the internet through such account or use such account as a phone line via VOIP.

441 Relief has not been granted in such terms in any previous known decision. The law knows of no sanction for copyright infringement other than that imposed by a court pursuant to Part V of the Copyright Act. Such sanction is not imposed until after a finding of infringement by a court. Such sanction is not imposed on anyone other than the person who infringed. Such sanction sounds in damages or, if criminal, possible fines and imprisonment, not removal of the provision of the internet.

442 That is not to say that such consideration prevents a finding of authorisation in the present circumstances of itself, but it does provide further evidence that warning followed by suspension or termination is not a reasonable step in the circumstances and is therefore not a relevant power to prevent.

TELCO ACT

443 The respondent further argues that the Telco Act prohibits it from using either the AFACT Notices or its own information to identify subscriber accounts. Use of such information is a precondition to a warning and termination or suspension regime. Accordingly, the respondent submits, warning and termination or suspension cannot be a power to prevent. As discussed, such reasoning is known as the Telco Act defence. The Court considers that the Telco Act defence is a complicated and discrete issue, and it will be dealt with in Part E2 of the judgment.

CONCLUSION

444 The Court finds that the respondent had no relevant power to prevent the infringements which were occurring. In making such finding, as discussed at [418] above, the claim that the respondent has authorised the infringements of the iiNet users must fail.

445 It is unfortunate that the outcome of the Court's finding is that the applicants will continue to have their copyright infringed. However, the fault lies with the applicants for choosing the wrong respondent. The current respondent does not stand in the way of the applicants pursuing those who have directly infringed their copyright nor in the way of the applicants pursuing any of the constituent parts of the BitTorrent system for authorisation. This decision in no way forecloses the applicants pursuing those other avenues to obtain a suitable remedy. The existence of infringement of copyright, however regrettably extensive, can never compel a finding of authorisation.

Section 101(1A)(b) Relationship

446 The second statutory consideration is *'the nature of any relationship existing between the person [the alleged authoriser] and the person [the primary infringer] who did the act concerned*'.

447 In the present circumstance it cannot be doubted that there is a direct relationship between the respondent and the owners of the accounts upon which the infringements occur. That relationship is a contractual one pursuant to the CRA. There is a non-contractual and more distant relationship between those who use accounts to infringe but are not directly subscribers of the respondent. Those persons are not contractually bound to the respondent, but there is still a relationship that is closer than that between Comcen and the unknown persons who used Mr Cooper's website in *Cooper*, for example, which was considered to be a relationship for the purposes of s 101(1A)(b) by Kenny J in *Cooper* 156 FCR 380 at [156]. However, the mere existence of the contractual relationship, given the preceding discussion, does not persuade the Court to change its finding regarding authorisation.

448 The Court accepts that there is a relationship between the respondent and its subscribers who were infringing copyright. However, the existence of a relationship does not compel a finding of authorisation. In *Australian Tape Manufacturers* the vendors had a direct

contractual relationship with those to whom they sold tape and recorders. The Adelaide Corporation had a direct contractual relationship with those who infringed in that decision. Yet in neither of these circumstances was authorisation established.

449 Both Branson J (at [46]-[48]) and Kenny J (at [150]) in *Cooper* 156 FCR 380 placed weight in the commercial aspect of the relationship between Mr Cooper and those infringing. The commercial relationship between infringers and authoriser was also a relevant consideration in *Cooper* 150 FCR 1 at [117] and in *Kazaa* at [404]. In the case of both Mr Cooper and the respondents in *Kazaa* it was found as a matter of fact that there was a direct relationship between the financial interest of the authoriser and the infringements which were occurring. In *Kazaa*, Wilcox J found at [191] and [404] that given that the Kazaa system was largely supported by advertising (few subscribers paying for a version without advertising), it was in the interests of the respondents to have as many people using the system as possible, and such imperative operated in the context that the predominant use and perception of use of the Kazaa system was as a tool of infringement. The same considerations applied in *Cooper*.

450 The Court finds that much more complex considerations arise in the present proceedings for two reasons. The first reason is that, as already discussed above at [239]-[250], despite their best efforts, the applicants have simply not proven that bandwidth use, downloading or quota use is, ipso facto, infringing. There are multiple uses for the internet and there are multiple means to consume significant amounts of quota for non-infringing purposes. Even where there is evidence before the Court of accounts where infringing activity is occurring, the evidence does not suggest that a significant amount of quota was being used for the purpose of infringing the applicants' copyright.

451 However, even if that finding be wrong, and there is a correlation between downloading, bandwidth and quota use and 'infringing activity', this does not lead to the conclusion that it is necessarily in the respondent's financial interests for the iiNet users to infringe as discussed at [224]-[238] above. The evidence of Mr Buckingham suggests that, at least within each subscriber plan, it is not in the respondent's interests for subscribers to use a substantial amount of monthly quota, given that the respondent's revenue from a subscriber is fixed but bandwidth is a variable cost. It was further shown on the evidence before the Court in the form of the RC-20 accounts and general statistics regarding the number of subscribers

of the respondent signed up to high quota plans that it is not necessarily apparent that most subscribers are upgrading their plans on the basis of their quota being used up and being shaped. Therefore, it was not necessarily in the respondent's interests to have the iiNet users using ever increasing amounts of bandwidth: see [233]. Further, it was shown (at [235]) that in relation to the sample of those who had infringed, the RC-20 accounts, such infringers were not the ideal subscribers of the respondent given that they regularly used their quota without necessarily upgrading their plans.

452 There is simply no sufficient nexus between profitability and the commercial interests of the respondent on the one hand and infringing activity on the other, such that it is necessarily in the respondent's interests to have the iiNet users infringing. Of course the respondent profits from infringements in an absolute sense, in that some of its subscribers are infringing and it is taking money from them. However, this was not a commercial interest in the same sense that was relevant for the purposes of the consideration of s 101(1A)(b) in *Kazaa* and *Cooper*.

453 In summary, the Court considers that while there is a relationship between the respondent and those who are infringing, such relationship of itself does not persuade the Court that the respondent is authorising the infringements of the iiNet users.

Section 101(1A)(c) Reasonable steps

454 The final statutory consideration is whether the alleged authoriser '*took any other reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice*'. It is agreed between the parties that there is no relevant industry code of practice.

WHAT IS THE ROLE OF REASONABLE STEPS?

455 As discussed above at [374], pursuant to the reasoning of Gibbs J, 'reasonable steps' becomes relevant only *after* the facts giving rise to authorisation have been established (at 14): '*if a person who was allowed to use the library made a copy of a substantial part of a book taken from the open shelves of the library…it can be inferred that the University authorized him to do so, **unless** the University had taken reasonable steps to prevent an infringing copy being made*' [emphasis added]. Based upon Gibbs J's reasoning, the

university's provision of, and control over, the photocopiers and library books in the library, coupled with its knowledge that infringements were likely to occur meant that it would authorise any infringement that resulted from the use of the copiers to copy library books, absent steps taken to prevent those infringements occurring. Following Gibbs J's analysis of authorisation, the place of reasonable steps is to remove a circumstance or conduct which would constitute authorisation of copyright infringement out of such context. In that sense, it operates as somewhat of a 'defence' or exculpation to authorisation. However, as also already discussed at [421], there is an inextricable link between the power to prevent infringement and reasonable steps. A step that is not reasonable will not constitute a relevant power to prevent infringement. This is demonstrated by the extract above: '*reasonable steps to prevent*…'. On Jacob J's analysis reasonable steps taken to prevent infringements occurring would be relevant as evidence to show that the implied invitation was relevantly qualified, such that it did not extend to using facilities to carry out copyright acts without licence.

456 It appears, however, that an analysis of reasonable steps now has relevance beyond its role as a 'defence' or exculpation to authorisation. In accordance with Gibbs J's reasoning, it would appear the failure to take reasonable steps would be, at the most, neutral to a finding of authorisation, in that it would merely deprive an alleged authoriser of a 'defence' to authorisation. But more recent authority has used the failure to take reasonable steps that could be taken as further evidence of authorisation. That is, an analysis of reasonable steps itself can be evidence of authorisation. The Court discussed such issue in making an earlier finding during these proceedings relating to an evidentiary dispute regarding whether, amongst other things, the evidence of the actions of other ISPs such as Telstra or Optus were relevant to these proceedings. The Court finds it is instructive to extract a portion of the informal reasons given to the parties:

> The Applicants are incorrect in their propositions advanced in paragraph 12 and 13. The inquiry is *unequivocally not* just into the steps taken by iiNet and whether they were reasonable. The Court is required to consider what reasonable steps *could* be taken by iiNet, and whether the absence of taking those steps might lead to an inference that iiNet authorised the infringing acts which occurred in the absence of those steps being taken.
>
> Such inquiries were made in *Cooper*, both at first instance and on appeal. For example, in *Cooper* at first instance, Tamberlin J said at [87]:-
>
> > However, **no attempt was made** by Cooper, when hyperlinks were submitted to the website**, to take any steps to ascertain the legality of the MP3s** to which the hyperlinks related or the identity of the

> persons submitting the MP3s. In the words of Knox CJ in *Adelaide Corp v Australasian Performing Right Association Ltd* (1920) 40 CLR 481 at 488, as approved by Gibbs CJ in *Moorhouse* at 13, Cooper "**abstained from action** which **under the circumstances then existing** it **would have been reasonable to take**, or ... exhibited a degree of indifference from which permission ought to be inferred."

Also, [121]:-

> Pursuant to s 101(1A) of the Act, in determining whether a person has authorised an infringement of copyright, the Court must take into account the extent of that person's power to prevent the doing of the act concerned and **whether that person took any other reasonable steps** to prevent or avoid the doing of the act…**They could have taken the step of taking down the website**.

Such extracts show that Tamberlin J (upheld by the Full Court) made a finding of what reasonable steps *could* have been taken by Cooper or the ISP, and that the finding of the failure to take that action was relevant to a finding of authorisation.

On appeal the Branson J (with whom French J agreed) in *Cooper* at [64] said:-

> E-Talk could have, but did not, take reasonable steps to prevent or avoid the doing of the acts of infringement (s 101(1A)(c)). Rather than withdrawing hosting of Mr Cooper's website, or otherwise placing pressure on Mr Cooper to stop his website being used for the predominant purpose of copyright infringements, E-Talk sought to achieve a commercial advantage from advertising on Mr Cooper's website.

And at [71]:-

> …Nor did the evidence suggest that there was **any reasonable step open to be taken** by Mr Takoushis personally to prevent or avoid the doing of the acts of copyright infringement. **While it would have been a reasonable step** for Mr Takoushis' employer to have **terminated its hosting of Mr Cooper's website, either absolutely or unless he removed the hyperlinks on it which facilitated copyright infringement**, the evidence **did not establish that Mr Takoushis had the necessary authority to do so himself** (s 101(1A)(c)). **I do not consider that it would have been a reasonable step for Mr Takoushis to approach his employer to compel them to do so.**

Kenny J (with whom French J also agreed) said at [167]:-

> …Mr Takoushis **was unable to cause** E-Talk to take down the website and discontinue its hosting arrangements with Mr Cooper. …. His superiors, such as Mr Bal, already knew about the website operated by Mr Cooper and the copyright difficulties to which it was likely to give rise; **and there was no other reasonable step that he could take to prevent the infringements.** In these circumstances, Mr Takoushis cannot be said to have relevantly "authorized": the doing in Australia of acts infringing the Record Companies' copyright.

All the judges on appeal therefore made an enquiry not only into the steps that *were* taken, but into steps that *could have been* taken and *would have been reasonable* to

> take. These findings led directly into the analysis of whether the actions taken or the absence of actions that could have been taken to have demonstrated authorisation on the part of the alleged authoriser. The enquiry of what is a reasonable step that could be taken necessarily requires a wider factual matrix than merely deciding whether specific acts that were positively made were reasonable steps to attempt to prevent or avoid copyright infringement. The Court may consider that iiNet could have taken a particular step, and that the absence of that step suggests iiNet was authorising the infringement that resulted because a failure to take that step. It is only fair that iiNet be able to provide evidence to submit that not only couldn't they take the step (for example, resulting from the prohibitions contained in the *Telecommunications Act 1997*) but also that, *in the circumstances*, it would not be reasonable to take a step even if they, strictly speaking, could take it. The Court is entitled to review evidence relating to those *circumstances*. [emphasis added in each of the above extracts]

457 There was also debate in these proceedings upon the question of which party was required to bear the evidentiary onus in relation to reasonable steps. That is, whether it was for the applicants to establish the reasonable steps the respondent could have taken to prevent the infringements of the iiNet users, or whether that was a matter for the respondent to prove. The answer is that both applicant and respondent may have the onus, depending on the point being made. As discussed, 'reasonable steps' in s 101(1A)(c) can act as a defence to authorisation as well as further evidence of authorisation. Therefore, if an applicant relies on reasonable steps that were not taken by an alleged authoriser as evidence of authorisation, the onus of proof of those steps not taken lies with the applicant. If a respondent seeks to show that it did take reasonable steps and therefore should not be found to have authorised, the onus of proof lies upon the respondent to prove that fact.

WERE THERE REASONABLE STEPS THE RESPONDENT COULD HAVE TAKEN?

458 The Court has made its findings in regards to whether the respondent had the power to prevent the infringements committed by the iiNet users. As found, the only relevant power to prevent was a scheme of notification and termination/suspension of subscriber accounts. The Court has found that such step was not a reasonable step.

459 As already discussed, there was insufficient evidence before the Court as to other technical steps that could have been taken but were not taken. The primary evidence on the subject of 'play-penning' and website blocking as a step to prevent copyright infringement related to the RC-20 accounts. They showed that the respondent had the ability to restrict subscribers' internet access where accounts were suspended for non-payment of fees to the respondent's website only, such that they had the ability to check their account details and

pay their account fees but do no more. However, that is insufficient evidence to prove that it would be technically possible for the respondent to implement such block on all subscriber accounts, and particularly the technical feasibility of blocking specific websites (rather than all websites except for one, which was the evidence before the Court). Even if it were technically possible, Mr Malone said that website blocks can be '*trivially bypassed*'.

460 Even more important than the technical availability of such step is a consideration of its scope. The AFACT Notices did not indicate that the copyright owners were suggesting that certain websites should have been blocked by the respondent. Rather, the information provided by such Notices to the respondent related to the actions of the iiNet users, and implied that action should be taken against the respondent's subscribers. The respondent was not provided with any guidance or information on any websites which were sought to be blocked by the applicants or AFACT. Such information is not self-evident, yet if action upon the AFACT Notices was sought, this was clearly an important consideration. It might be expected that the blocking of a website ought to be considered a serious step, given the nature of the internet as an open platform to communicate. Mr Malone testified that it was not the respondent's practice to block any websites, no matter how nefarious. Consequently, any claim that a failure to block would be construed as authorisation ought to have been distinctly made and proved to the respondent. Absent such details it could not be said that the respondent's failure to do so was evidence of authorisation.

Other considerations – Knowledge of infringements

461 There can be no doubt that the mere insertion of s 101(1A) into the Copyright Act was not intended to prevent the Court from considering matters other than those mentioned in s 101(1A)(a)-(c) when considering whether authorisation of infringement is made out. Knowledge of infringements is one such consideration: see, for example, *Kazaa* at [370]; and *Metro* at [46]-[52].

462 Following the introduction of the *Copyright Amendment (Digital Agenda) Bill 1999* ('*Copyright Amendment (Digital Agenda) Bill*') a recommendation was made by the House of Representatives Standing Committee on Legal and Constitutional Affairs that an additional consideration be inserted into the s 101(1A) considerations, namely '*whether the person knew the infringing character of the act or was aware of facts or circumstances from which the*

infringing character of the act was apparent'. The *Copyright Amendment (Digital Agenda) Act* did not incorporate such recommendation. However, this does not lead to the conclusion that knowledge is not a relevant consideration.

463 The role of the knowledge held by the alleged authoriser of the occurrence of infringements is an important consideration, but the existence or lack thereof of that knowledge does not compel a finding either way on the question of authorisation.

464 Pursuant to Jacobs J's reasoning in *Moorhouse*, knowledge of infringements occurring is irrelevant as long as there is an unqualified implied or express invitation extended to the primary infringer to use the facilities offered to infringe (see *Moorhouse* at 21). Adopting Gibbs J's reasoning, knowledge is necessary, given that one must provide the 'means' of infringement '*knowing, or having reason to suspect*' (at 13) that it is likely to be used to infringe. Accordingly, it is uncertain whether authorisation can be made out if there is no knowledge or suspicion that there are acts of primary infringement occurring. The mere existence of knowledge will not mandate a finding of authorisation either, '*[k]nowledge that a breach of copyright is likely to occur does not necessarily amount to authorisation, even if the person having that knowledge could take steps to prevent the infringement*: Australian Tape Manufacturers Association Ltd v Commonwealth (1993) 176 CLR 480 at 497-498' *Nationwide News Pty Ltd and Others v Copyright Agency Limited* (1996) 65 FCR 399 ('*Nationwide News*') at 424 per Sackville J speaking for the Full Court. Such statement has been approved in *Nominet* at [129]; *Cooper* 156 FCR 380 at [31] per Branson J, [144] per Kenny J; *Kazaa* at [370]; and *Cooper* 150 FCR 1 at [80].

465 The respondent has accepted that it had general knowledge of copyright infringement committed by iiNet users or that infringement was likely to occur on its facilities. However, at such a level of abstraction it is very difficult to act on such knowledge in any meaningful way. Accordingly, the Court considers that it would be difficult to make a finding of authorisation on that level of knowledge alone. In this sense, s 101(1A)(a) and (c) considerations interact with the issue of knowledge in considering a finding of authorisation. For example, in some circumstances a relevant power to prevent will be to refrain from offering a facility by which infringements could occur, such as when the facility is calculated to lead to its use to infringe copyright (as discussed above at [419]). In such circumstance,

knowledge, at an abstract level of likelihood of infringements, will be sufficient. However, where it would not be a reasonable step to refrain from offering any facilities by which infringements might occur, such as in the present case in which no claim has been made that the respondent should shut down its operations as an ISP, but a more specific step could be taken, it would appear to be necessary that to make a finding of authorisation the level of knowledge of the alleged authoriser be sufficiently specific to take that step. In the present circumstances the Court has found that the only possible reasonable step or power to prevent would have been for the respondent to notify and then terminate or suspend its subscribers for infringing. Therefore, the relevant level of knowledge would have to be at this level of specificity. In the present proceedings the only evidence at that level of specificity is the AFACT Notices.

466 The Court finds Mr Malone and Mr Dalby were honest in stating that they did not understand all the technical detail of the spreadsheet attached to the AFACT Notices and the DVD attached. The Court notes that the headings to the columns included in the spreadsheet attached to the AFACT Notices were not self-evident. Nor was the information found on the DVDs. Mr Carson did not appear to have difficulty in understanding the data (as discussed in his second report), but he had already prepared his first report explaining in detail how the BitTorrent protocol functioned. That report was predicated on Mr Carson having '*reviewed and collated information from Internet based resources, including knowledge based web sites, blogs and postings*'. That is, Mr Carson, an expert in computer forensics particularly related to copyright infringement, had to research the topic extensively before he was able to provide his report on the subject of the information attached to the AFACT Notices, and was therefore in possession of the required level of comprehension of the detail contained in the AFACT Notices, spreadsheets and DVDs.

467 Mr Malone was aware of the BitTorrent protocol only in very general terms, and Mr Dalby did not appear to have any knowledge other than such protocol's mere existence. Of course Mr Malone and Mr Dalby would have understood the gist of what the AFACT Notices were alleging, as Mr Parkinson wrote to AFACT in the second email dated 12 August 2008, '*IiNet understands how AFACT has come to its allegation of copyright infringement based on an IP address, date & time*', but that level of appreciation is different from knowing *how*

such allegations came to be made, that is, how those IP addresses, dates and times were generated.

468 The 29 July 2008 response from AFACT to the respondent's response to the first AFACT Notice stated '*[g]iven iiNet is presently the third largest ISP in Australia, it would have no shortage of technically qualified employees who should have no difficulty understanding the information provided to iiNet by AFACT*'. Such observation was likely to be correct. However, given the context whereby ISPs such as the respondent had received, and continue to receive, thousands of notices of infringement from overseas (in the form of the 'robot' notices discussed at [192] which the Court cannot find to be reliable) and previous mechanisms to inform ISPs of infringements occurring, such as those using Media Sentry, had been shown to be unreliable, there was an obligation on AFACT to make clear that their data was different if they expected a positive response. The draft 'straw man' response to AFACT created by Mr Perrier of Telstra (see [201] above) and sent to the diss_connect group attached an academic paper from the University of Washington. The academic paper became exhibit KK. Such paper explained why the investigative mechanism of Media Sentry was flawed, and could lead to false allegations of copyright infringement. Given that email, it would appear that none of the ISPs in the diss_connect group, including the respondent, appreciated the distinction between Media Sentry's investigative mechanisms and that of DtecNet.

469 The Court has before it a partially confidential report of Mr Lokkegaard explaining in great detail how his computer software, the DtecNet Agent, operates. The Court has a report of Mr Carson *independently* confirming the accuracy of the DtecNet method. Both provide extensive and, in some cases, confidential detail, and in the absence of such information the operation of the DtecNet Agent could not necessarily be understood. Yet the respondent had neither report at the time when the AFACT Notices began arriving. The Court finds that AFACT should have explained, in providing the AFACT Notices, how the allegations of infringement came to be made in detail, that is, how the DtecNet Agent operated. DtecNet (and therefore AFACT) is not entitled to keep its method secret while at the same time expecting ISPs and others to be convinced of the reliability of the allegations of infringement it creates and to therefore act on those allegations. The applicants certainly have not expected the Court to take the DtecNet evidence at face value. They have explained and proven both

the method of evidence gathering and used an expert to independent verify its veracity. This was exactly the point of the respondent's response to AFACT: it wanted an independent third party to assess the reliability and authenticity of such evidence. There was nothing unreasonable in the respondent taking such a position.

470 Mr Malone's statement referring to the AFACT Notices being '*compelling evidence*' does not change the Court's finding. Mr Malone's use of that statement, as already discussed, was expressly qualified in that he made such statement in the context of that evidence being reviewed by a third party such as this Court.

471 Despite the foregoing, it can be accepted that from some point after the commencement of the present litigation the respondent gained the relevant level of knowledge that enabled it to act, and it became aware of the manner in which the DtecNet evidence was gathered. That is, whatever its knowledge in 2008, at some point after the commencement of litigation the respondent possessed knowledge which enabled it to act as this cross-examination of Mr Malone showed:

> Well, you know it is happening and know it has happened, correct, since at least April 2009?---Based on these documents, yes.
>
> And your response has been to give them [iiNet users] further access?---Correct, subject to the outcome of this litigation.

472 However, the Court does not find such conclusion determinative. As extracted above at [465] mere knowledge, as well as the power to prevent is not, ipso facto, authorisation. For all the reasons already outlined in the discussion of the 'means' of infringement as well as s 101(1A)(a)-(c) of the Copyright Act, the Court finds that authorisation is not made out in the present circumstances, despite the respondent's knowledge of the infringements occurring.

Other considerations – Encouragement of infringement

473 The applicants point to acts of the respondent which are submitted to be positive encouragement to iiNet users to infringe. Wilcox J found at [405] of *Kazaa* that Sharman positively encouraged copyright infringement on its Kazaa system. As discussed above at [391] the very design of Mr Cooper's website encouraged infringement and it was set up for that purpose.

474 The actions of the respondent relied upon by the applicants which allegedly encouraged infringement are: firstly, failing to take any action to prevent the infringements; secondly, a 20 November 2008 press release; thirdly, the means by which that press release was disseminated; fourthly, the '*Golden Girls* advertisement' and finally the respondent's encouragement to its subscribers to upgrade their plans.

Failure to act

475 The first example, the failure of the respondent to take any action to stop infringements occurring, is not encouragement of infringement. At the outset, the Court has found that the action suggested was not a relevant power to prevent or reasonable step and thus did not need to be taken. Regardless, failure to discourage copyright infringement is not encouragement of copyright infringement. There is a middle ground, namely remaining neutral as the respondent did. On this basis, the Court rejects this claim.

20 November 2008 press release

476 The second example is not encouragement either. The applicants point to the 20 November 2008 press release (exhibit U) by the respondent regarding the institution of these proceedings. The relevant section extracted by the applicants is:

> "iiNet cannot disconnect a customer's phone line based on an allegation. The alleged offence needs to be pursued by the police and proven in the courts. iiNet would then be able to disconnect the service as it had been proven that the customer had breached our Customer Relations Agreement," Mr Malone said.

The applicants have argued that as Mr Malone had accepted during his cross-examination that infringements had occurred, it was incumbent upon the respondent to at least amend or clarify such press release. The Court rejects the argument. The Court takes judicial notice of the fact that these proceedings have generated numerous press releases from both the applicants (via AFACT) and the respondent. Such press releases were released by the parties for purposes ulterior to providing all the relevant information to the public. Their purpose was 'spin' and they are, as such, unreliable. However, that does not mean that this release would constitute encouragement to infringe if it were not amended or subsequently clarified.

477 The statement referred to above appears to remain the position of the respondent. It may have accepted, for the purpose of this trial, that the AFACT Notices proved certain types

of copyright infringement, but the respondent's statement would still be pertinent to that context. The statement specifically says, '*[t]he alleged offence needs to be…proven in the courts*'. Such offence, namely copyright infringement, was not proven in this Court until the handing down of this judgment. Mr Malone's reference to '*compelling evidence*' as discussed above at [172]-[180] was in the context of that evidence being tested in Court.

478 Further, even if that were not the case, the press release related to the respondent choosing to defend itself against the allegation that it had authorised the infringement of copyright. To suggest that defending oneself against such allegation, and explaining its position to the public, could itself constitute an encouragement to the iiNet users to infringe which would support a finding of authorisation, is absurd.

479 The applicants submit that the option of downloading such press release via the BitTorrent system was further encouragement to infringe. The Court can make no such finding. The mere use of the BitTorrent system of itself does not infringe copyright. Consequently, the provision of such press release via BitTorrent, while unusual, was not an encouragement to the iiNet users to infringe.

'Golden Girls *advertisement*'

480 The applicants submit that the following radio advertisement was an encouragement by the respondent to the iiNet users to infringe:

> [t]o internet users a Gig is a Gigabyte. The question is, how big is a Gig? A Gig is about 500 hi-res photos or about 300 songs or 5 episodes of the *Golden Girls*. At iiNet we explain all this to you so you can choose a broadband plan that's right for you … it's not the size of the Gig, its how you choose to use it.

481 The Court believes the following finding of Gummow J in *Hanimex* at 288 is apposite:

> The respondent submits that particularly when the advertisements in question are listened to rather than their text read, the general impression is one of promotion of the virtues of the physical properties of the respondent's product in comparison with the properties of other products…In my view, the substance of the colourful and somewhat exaggerated language of the advertisements is not an invitation or incitement to or approval of the reproduction of the sound recordings by Madonna for which copyrights are held by the applicants.

482 There is evidence of the availability of television programs for download or streaming on the internet which are perfectly legitimate and not in the Freezone: see [245]. It would be useful for non-technically minded people to know how much quota would be used up by activities that they might undertake on the internet. The reference to *Golden Girls* was clearly intended to be humorous given its somewhat less than contemporary relevance. Indeed, the joke is that it is highly *unlikely* that someone would download an episode of the *Golden Girls*. It is not an invitation to download the *Golden Girls*. Rather, it is a tongue-in-cheek reference to a section of popular culture. The Court does not understand why Mr Malone found it necessary to be so apologetic about the advertisement in his cross-examination.

483 As mentioned, Wilcox J considered that some advertising of the respondents in the *Kazaa* decision constituted encouragement to people to infringe copyright via the Kazaa system. To appreciate how utterly innocuous the '*Golden Girls* advertisement' is in comparison, it is instructive to extract the advertisement as referred to by Wilcox J (from *Kazaa* at [178]):

THE
KAZAA
REVOLUTION
30 years of buying the music of [sic] they think you should listen to.
30 years of watching the movies they want you to see.
30 years of paying the prices they demand.
30 years of swallowing what they're shovelling.
30 years of buying crap you don't want.
30 years of being a sheep.
Over. With one a single click.
Peer 2 peer, we're sharing files.
1 by 1, we're changing the world.
Kazaa is the technology.
You are the warrior.
60 million strong. And rising.
Join the revolution
KAZAA
Share the revolution

484 As Wilcox J found at [405] '*[e]specially to a young audience, the "Join the Revolution" website material would have conveyed the idea that it was "cool" to defy the record companies and their stuffy reliance on their copyrights*'. The '*Golden Girls* advertisement' was not even remotely similar in tone or intention.

Encouragement to upgrade

485 As outlined at [239]-[250] the use of bandwidth or quota or downloading is not necessarily copyright infringing. Therefore encouragement to use more bandwidth or quota, or to download more, cannot be encouragement to infringe.

486 The Court rejects each of the above examples relied upon as being evidence of encouragement to infringe.

Other considerations – Inactivity or indifference

487 Gibbs J in *Moorhouse* at 12 accepted the proposition from *Adelaide Corporation* that '*[i]nactivity or indifference, exhibited by acts of commission or omission, may reach a degree from which authorization or permission may be inferred*'. However, a precondition to a finding that a person is indifferent or inactive is a finding that action was warranted and required. That is, some obligation to act must exist for one to be properly characterised as inactive.

488 It is submitted that the respondent's failure to act on the AFACT Notices was evidence of this inactivity or indifference. The following extract of *Jain* at 61 was said to be relevant to the present circumstances:

> …the evidence in the present case reveals, in our opinion, a studied and deliberate course of action in which Mr Jain decided to ignore the appellant's rights and to allow a situation to develop and to continue in which he must have known that the appellant's music would be played without any licence from it. It was within his power to control what was occurring be [sic] he did nothing at all.

See *Metro* at [52] to similar effect.

489 Such finding of indifference was, necessarily, conditioned upon two matters. The first was '*the evidence in the present case*' and the second was '*[i]t was within his power to control what was occurring*'. It is dangerous to take statements such as the above out of the context in which they applied, that is, the facts before their Honours in those proceedings. Doing so can distract from the relevant enquiries in an analysis of authorisation, which, as stated in *Jain*, begin with *Moorhouse* and, following its introduction, s 101(1A) of the Copyright Act.

490 The Court accepts that the respondent knew that infringements were occurring or were likely to occur. The Court accepts that the respondent has not acted to stop those infringements. However, such considerations fail to account for the important first step in a finding of authorisation, that is, whether the alleged authoriser has provided the 'means' of infringement, not merely a precondition to infringement, and whether there is a relevant power to prevent infringement that could be exercised by the alleged authoriser. As mentioned, the reasoning above was expressly conditioned on it being within Mr Jain's control or, in s 101(1A) parlance, his power to prevent the infringements occurring. In the present proceeding the respondent has neither provided the 'means' of the infringement nor has the power to prevent those infringements, and in the absence of these essential pre-conditions, indifference is irrelevant.

491 It is instructive to extract a statement of Higgins J from *Adelaide Corporation* at 497:

> At most, it might be said that the Corporation showed itself indifferent; but, as "indifference" has a rather dyslogistic sense, let us say that the Corporation remained neutral. The problems involved in the letter of 7th October called for consideration and caution: and the Corporation had not the function of policing the provisions of the *Copyright Act* on behalf of alleged owners of copyright.

492 There is no legal obligation or duty on any person to protect the copyright of a third party. There is only a legal prohibition on doing an act composed in the copyright without the licence of the owner or exclusive licensee of that copyright or authorising another to do that copyright infringing act. Consequently, merely being indifferent or inactive in the knowledge that copyright infringement is occurring cannot possibly constitute authorisation. A key factor which must be present is control, or the power to prevent. But, of course, even that may not be enough, as was found by the Full Court in *Nationwide News* at 424 as extracted above at [464].

Did the respondent sanction, approve, countenance the infringements of the iiNet users?

493 It has been accepted in virtually every authorisation decision from *Adelaide Corporation* onwards that the word authorisation has the Oxford Dictionary meaning of '*sanction, approve, countenance*': see *Falcon v Famous Players* at 474; *Adelaide Corporation* at 489; *Moorhouse* at 12, 20; *Hanimex* at 286; *Jain* at 57; *Nationwide News* at 422; *Metro* at [16]; *Cooper* 150 FCR 1 at [78]; *Kazaa* at [402]; and *Cooper* 156 FCR 380 at [20], [138]. Therefore, despite all the preceding discussion and authority on the issue, at its

heart, the question of authorisation is a simple question of fact, answered by the following: did the alleged authoriser sanction, approve, countenance the infringements which occurred?

494 It is to be noted that the judicial authority refers to all three words (sanction, approve, countenance) together, separated by commas and therefore all are to be considered. That is, the inquiry is not whether the alleged authoriser sanctioned, approved *or* countenanced the infringement, it is whether they sanctioned, approved, countenanced the infringement.

Approve

495 As to the word 'approve', the Oxford Dictionary defines such word as meaning, '*to pronounce to be good, commend*'. Such definition, particularly the word '*pronounce*' suggests that approval will only be found where there is some positive announcement of approval of infringements occurring. However, it is clear from *Moorhouse* at 12; *Hanimex* at 286; and *Metro* at [19] that, '*active conduct indicating approval [is] not essential to a finding of authorisation*'. In *Cooper* 150 FCR 1 Tamberlin J found at [84] that '*Cooper…knowingly…approved the use of his website in this manner [a copyright infringing manner] and designed and organised it to achieve this result*'. Such finding was upheld on appeal. In *Kazaa* at [194] Wilcox J found similarly regarding the Kazaa system.

Sanction

496 As to the word 'sanction', the Oxford Dictionary defines such word as meaning '*to permit authoritatively; to authorize; in looser use, to countenance, encourage by express or implied approval*. Tamberlin J and Wilcox J found at [100] and [194] of *Cooper* 150 FCR 1 and *Kazaa* respectively that the respondents sanctioned the infringement.

Countenance

497 As to the word 'countenance', the Oxford Dictionary defines such word as meaning *'to give countenance to; to look upon with sanction or favour; to favour, patronize, sanction, encourage…a thing*'. In *Jain* at 61 the Full Court said:

> [t]he judgment of the members of the High Court in the *Moorhouse* case establishes that one of the meanings of the word "authorise" in the context in which it is here used is "countenance". It may be that not every act which amounts to the countenancing of something is an authorisation. Every case will depend on its own facts. Matters of degree are involved.

Branson J adopted such statement in *Cooper* 156 FCR 380 at [72]:

> It may be that Mr Takoushis can be understood to have "countenanced" the acts of copyright infringement in the sense that he supported or showed favour to those acts (see *The Macquarie Dictionary* (2nd ed)). However, as the Full Court observed in [*Jain*] every case in which the issue of whether a person authorised an act of copyright infringement arises will depend on its own facts and involve matters of degree.

498 Branson J also found in that decision at [65] that Comcen, at the least, countenanced the infringements which occurred by means of Mr Cooper's website. Kenny J found at [152] and [158] that both Mr Cooper and Comcen countenanced the infringements occurring by means of Mr Cooper's website. In *Metro*, Bennett J found at [52] that Metro had countenanced the infringements that occurred at its venue. In *Kazaa*, Wilcox J found at [194] that Sharman and Altnet countenanced the infringements which occurred by means of the Kazaa system.

499 It was put to Mr Malone that he countenanced the infringements of the iiNet users, particularly RC-08, one of the RC-20 accounts:

> Your company is countenancing that customer continuing to infringe copyright, isn't it?---No. Countenancing implies some form of approval of it. I certainly don't approve of what he's doing or she's doing.
>
> Well, if you don't approve why don't you stop them getting access to the internet?---We would have if there had been a requirement-if that could have been part of the orders here as well is to provide that information and disconnect we would have immediately acted on it.
>
> But you know they only infringe if you provide them access, but you continue to provide them access. Correct?---They could continue to infringe by any other means.
>
> But you know that the claimed act of infringement is the making available online through your customer's account on your service. You know that, don't you?---Yes.
>
> And you know that the only way they can continue to do that that is if you keep-continue to provide them with access. Correct?---Yes.
>
> You are countenancing them infringing, are you not?---Again, I say by the word countenance you mean approving of it, no I don't.

Findings

500 Consistent across all the words 'approve', 'sanction' and 'countenance' is the element of approval or favour with what is said to be authorised, whether it be explicit or to be implied. There appears to be a consideration that 'countenance' is of a lesser force than that

of 'approval' in assessing whether particular factual circumstances give rise to behaviour or conduct which authorises, in the sense that approval of infringement will almost always suffice for a finding of authorisation. However, countenancing may not: see *Jain* at 61.

501 In the current proceedings, the Court does not find that the respondent approved or sanctioned or even countenanced the copyright infringements of the iiNet users. All terms imply a sense of official approval or favour of the infringements which occur. Such approval or favour cannot be found.

502 Mr Malone has made public statements that copyright infringement is wrong. For example, on the Whirlpool forums on 29 March 2005 and 31 March 2005 and to the media on 29 March 2005 and during the proceeding. The respondent publicly stated in the 20 November 2008 press release that '*iiNet does not in any way support or encourage breaches of the law, including the infringement of copyright*'. This statement was repeated in 17 December 2008 and 5 February 2009 press releases regarding these proceedings. The respondent has implemented a CRA that prohibits subscribers from using their internet to infringe copyright.

503 Of course these public statements would count for nothing if it was apparent that in reality the respondent tacitly approved of copyright infringement. For example, the public pronouncements and notifications telling people not to infringe copyright in *Kazaa* and *Cooper* did not reflect the reality of the situation. In those decisions the authoriser intended that the 'means' of infringement be used to infringe – clearly sufficient to make out that they approved or favoured infringement. The Court can find no similar evidence in the present circumstances. The respondent does not intend, and has never intended, that its facilities be used to infringe. In fact it implemented the Freezone which is a net cost, and which provides an attractive mechanism for iiNet users to consume media, including the applicants' media, in a way which does not infringe copyright.

504 It cannot be doubted that the respondent did not do what was demanded of it by AFACT. However, this approach is not the same as approving of infringements. The applicants appear to premise their submissions on a somewhat binary view of the world whereby failure to do all that is requested and possible to co-operate with copyright owners to stop infringement occurring, constitutes approval of copyright infringement. Such view is not

the law. It is possible to be neutral. It is possible to prefer one's own interests to those of the copyright owners. As Higgins J found at 497 in *Adelaide Corporation*, the law recognises no duty to police copyright infringement for the benefit of third parties. The law merely prohibits authorisation of copyright infringement. The law recognises that favour may be implied from inaction. However, this is only so where action could or should be taken. For all the reasons discussed in this part of the judgment the respondent was not required to act and its inaction did not equal favour. It did not sanction, approve, countenance the copyright infringement of the iiNet users.

Conclusion on authorisation

505 The Court accepts the respondent had knowledge of the infringements occurring. The Court accepts that it would be possible for the respondent to stop the infringements occurring. However, the Court has found as a matter of fact that the respondent did not authorise the infringement committed by the iiNet users. Such finding is premised on the fact that the respondent did not provide the 'means' by which those iiNet users infringed. Even if that finding be wrong, the Court finds that while the respondent could stop the infringements occurring in an absolute sense, the steps to do so were not a power to prevent the infringements or a reasonable step in the sense used in s 101(1A)(a) or (c) of the Copyright Act. Finally, the Court has found that the respondent did not approve, sanction, countenance the infringements committed by the iiNet users.

506 It follows that the present Amended Application against the respondent must fail.

507 However, despite such finding, the Court considers that it should make further findings in relation to the other matters that were argued before it. Therefore, the Court will move on to a consideration of the Telco Act defence, s 112E of the Copyright Act and finally the safe harbour provisions.

PART E2: THE TELCO ACT DEFENCE

508 As already mentioned at [443] above, the respondent argues that the Telco Act prohibited it from acting on the AFACT Notices and warning, suspending or terminating its subscribers for copyright infringement (the Telco Act defence). The respondent argues that if the Telco Act defence is upheld, it would operate as a complete answer to authorisation.

However, the respondent submits, if it be not upheld, authorisation would nevertheless not be found for other reasons. As the Court has found that the respondent did not authorise the infringements of the iiNet users, the Telco Act defence is redundant. Nevertheless, given the length of argument on the issue the Court considers that there is value in making findings on the issue.

509 The respondent argues that it would have to use three different kinds of information to bring about a warning/suspension/termination scheme. The first would be the provision of the IP addresses and times provided by the AFACT Notifications ('AFACT information'). The second would comprise information in the respondent's '*score*' database which contains information identifying those IP addresses which were allocated to particular subscriber accounts at certain times ('score information'). The third would consist of the information contained in the '*rumba*' database which contains the personal details (such as names, addresses, emails and telephone numbers) of its subscribers ('rumba information'). The respondent would have to match the AFACT information to the score information which would give it the subscriber account which was implicated in the alleged copyright infringement. Once it had that information it could then consult the rumba information which would contain the contact details of the owner of that subscriber account.

510 The respondent argues that the Telco Act prohibits the use of any such information for the purposes of warning its subscribers of allegations of copyright infringement and of termination of subscriber accounts for such reason. The respondent submits that upholding the Telco Act defence would operate to prevent the Court from making a finding of authorisation irrespective of whether such defence was in the minds of the employees of the respondent at the time of first receipt of the AFACT Notices. The Court concurs but, as will become apparent, the issue of whether the Telco Act defence existed at the time of the first receipt of the AFACT Notices is an irrelevancy, due to the Court's findings regarding the Telco Act defence.

The Telco Act

511 Section 270 of the Telco Act is contained in Division 1 of Part 13 of that Act. Such part is entitled '*Protection of communications*'. Section 270 provides a simplified outline of Part 13:

- Carriers, carriage service providers, number-database operators, emergency call persons and their respective associates must protect the confidentiality of information that relates to:

  (a) the contents of communications that have been, or are being, carried by carriers or carriage service providers; and

  (b) carriage services supplied by carriers and carriage service providers; and

  (c) the affairs or personal particulars of other persons.

- The disclosure or use of protected information is authorised in limited circumstances (for example, disclosure or use for purposes relating to the enforcement of the criminal law).

- An authorised recipient of protected information may only disclose or use the information for an authorised purpose.

- Certain record-keeping requirements are imposed in relation to authorised disclosures or uses of information.

512 As mentioned, it is agreed between the parties that the respondent is a carriage service provider ('CSP'). For all relevant purposes a CSP is the same as an ISP, but as the term CSP is used in the Telco Act, the Court will refer to the respondent as a CSP in this part.

Operation of s 276

513 Section 276 of the Telco Act relevantly provides:

(1) An eligible person must not disclose or use any information or document that:

(a) relates to:

(i) the contents or substance of a communication that has been carried by a carrier or carriage service provider; or

(ii) …

(iii) carriage services supplied, or intended to be supplied, to another person by a carrier or carriage service provider; or

(iv) the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(b) comes to the person's knowledge, or into the person's possession:

(i) if the person is a carrier or carriage service provider-in connection with the person's business as such a carrier or provider; or

(ii) …

514 Section 276(3) makes contravention of s 276 an offence:

Offence

> (3) A person who contravenes this section is guilty of an offence punishable on conviction by imprisonment for a term not exceeding 2 years.

515 The respondent claims, and it is not the subject of dispute, that, as a CSP, it is an '*eligible person*' within the meaning of s 271 of the Telco Act. Consequently, disclosure or use by the respondent of information that falls within s 276(1)(a) and (b) is prohibited, unless certain exceptions apply.

516 The Oxford Dictionary defines '*use*' as '*[t]o make use of (some immaterial thing) as a means or instrument; to employ for a certain end or purpose*'. The Court finds that were any of the AFACT information, score information or rumba information sought to be put to the purpose of notifying or terminating subscriber accounts, that would be relevant '*use*' of that information for the purpose of s 276. Therefore, the relevant question is whether the information sought to be used falls into s 276(1)(a) and then 276(1)(b).

Does the information required to be used satisfy s 276(1)(a)?

517 It is accepted by the applicants that the AFACT information satisfies s 276(1)(a)(i),(iii) and (iv). Consequently, the score information must necessarily also satisfy s 276(1)(a)(i),(iii) and (iv) because that information is relevantly the same as the AFACT information, being IP addresses and times. The rumba information, given that it comprises subscriber contact and personal details, can only sensibly satisfy s 276(1)(a)(iv). Therefore, all the information falls within s 276(1)(a).

Does the information required to be used satisfy s 276(1)(b)?

518 There is no issue that the score information and the rumba information fall into s 276(1)(b)(i). The relevant debate is whether the AFACT information satisfies s 276(1)(b)(i).

519 The wording of the section such that the information must come within the person's knowledge or possession '*in connection with the person's business as such a carrier or provider*' suggests a wide range of potential types of information, particularly the use of the word '*business*', which suggests wider circumstances than the mere technical process by which the respondent provides internet access to its subscribers. As Campbell J said at [7] in *C J Redman Constructions Pty Ltd v Tarnap Pty Ltd* [2006] NSWSC 173, '*the expression "in connection with", while sometimes capable of referring to a connection of any kind between*

two subject matters, does not always have that reference…[i]t is necessary to look to the context in which the expression occurs'. In this circumstance, the use of the word '*business*' provides important context to the term '*in connection with*'. It suggests a wide variety of connections.

520 The applicants submit that as the AFACT Notices collected publicly available information from swarms sharing particular files, that information cannot sensibly fall under s 276 and thereby give rise to an offence due to further disclosure or use of that public information. The applicants submit that such an outcome would not be pursuant to the purpose of the section.

521 Such submission is misconceived for two reasons. The first reason is that a significant amount of information which falls under s 276 would necessarily otherwise be public information. A person's name is public information. A person's address is public information. However, both examples, when provided to a CSP for the purposes of signing up to its services (as part of its business), clearly fall under s 276(1) and thus further disclosure or use is not permitted by that CSP except in certain circumstances. The purpose of s 276 is not to prohibit disclosure only of information which is not public.

522 The applicants' submissions are, in essence, that s 276 is designed to cover only information generated by the CSP, and information provided to the CSP by a subscriber. The Court can find no such limitation in the wording of the section, nor any purpose that would justify such a narrow interpretation of s 276. As stated, '*in connection with the person's business as such a carrier*' necessarily covers a wide range of information. The Court rejects the submission of the applicants that '*third party information*', namely information from a person other than the CSP or the subscriber, is excluded from the ambit of s 276(1)(b)(i).

523 The second reason is that the AFACT Notices do more than provide information; they provide information directed towards a particular purpose. The Notices are headed '*Notification of Copyright Infringement*', making that purpose clear. The AFACT information has been collated and sent to the respondent in its capacity as a CSP. The AFACT Notices demand that they be acted upon with the implication that the respondent should warn its subscribers or terminate its subscribers' access to the internet. Such demands are clearly a matter relevant to the respondent's business as a CSP. The information has only come into

the respondent's possession because of its business as a CSP. The AFACT Notices were not sent by AFACT to any other persons. Indeed, they could only be sent to a CSP because a CSP is the only person that could sensibly do anything with such Notices.

524 The origin of the information might have been public, being obtained from a swarm, but that information has been taken from the public context, converted into a much narrower context of alleging copyright infringement, and then sent to the respondent to act on. The information has clearly come into the respondent's possession in connection with the respondent's business as a CSP and thereby falls under s 276(1)(b)(i).

525 However, even if the Court be wrong in its finding in relation to the AFACT information falling under s 276, such finding is an irrelevancy. This is because in order to bring about the result the applicants demand, all three sources of information must be used, not just the AFACT information. Therefore, were the Court wrong in its finding regarding s 276 and the AFACT information, that information could be used without prohibition, but such information cannot be used to any end in isolation. It must be used with the rumba and score information which undoubtedly fall under s 276.

526 All the information in question falls under s 276 and its use or disclosure is prohibited unless some exception found in Division 3 of Part 13 of the Telco Act applies. If the Court be wrong in regard to its finding concerning the AFACT information, s 276 nonetheless prevents the use or disclosure of the score information or the rumba information.

Exceptions

527 Division 3 of Part 13 of the Telco Act provides the exceptions to the prohibition on the use or disclosure of information found in s 276 of the Telco Act. The four relevant exceptions for the present circumstances are ss 279, 280, 289 and 290. Each will be addressed in turn.

Operation of s 279

528 Section 279(1) of the Telco Act provides:

> **Performance of person's duties**
>
> (1) Section 276 does not prohibit a disclosure or use by a person of information or a document if:

> (a) the person is an employee of:
>
> (i) …; or
>
> (ii) a carriage service provider; or
>
> (iii) …; and
>
> the disclosure or use is made in the performance of the person's duties as such an employee.

529 The critical issue arising in the consideration of this question is whether the use of the information in the AFACT information as well as the score and rumba information would be made by an employee of the respondent '*in the performance of the person's duties*'. An employee's duties would presumably involve daily administration of a subscriber's account. But could it be said that the investigation of information provided by a third party concerning a possible infringement of that party's rights would constitute performance of the person's duties as such an employee?

530 In *Canadian Pacific Tobacco Limited and Another v Stapleton* (1952) 86 CLR 1 at 6 Dixon CJ, commenting on a provision of similar wording and intendment, said:

> [the provision] ought to receive a very wide interpretation. The word "duty" here is not, I think, used in a sense that is confined to legal obligation, but really would be better represented by the word "function". The exception governs all that is incidental to the carrying out of what is commonly called the "duties of an officer's employment"; that is to say, the functions and proper actions which his employment authorizes.

531 While the respondent has no duty to exercise its rights under the CRA, that does not mean that were it to do so it would not be protected by s 279. If, as part of an employee of the respondent's duties, an employee is required to investigate whether a subscriber is, or has been, engaged in conduct which is alleged to have breached the CRA, such investigation would be performed by the employee of the CSP and the three types of information would be utilised in the performance of their duties. The respondent would be conducting an enquiry, through its employee, to determine if its subscriber had complied with the CRA, and further to exercise its rights under that CRA.

532 Accordingly, the Court finds that the disclosure or use of the information is authorised by s 279 of the Telco Act.

Operation of s 280

533 Section 280 of the Telco Act relevantly provides:

> **Authorisation by or under law**
>
> (1) Division 2 does not prohibit a disclosure or use of information or a document if:
>
> (a) …; or
>
> (b) in any other case-the disclosure or use is required or authorised by or under law.

534 The applicants submit that as s 101 of the Copyright Act creates a tort of authorisation of copyright infringement this must mean that use of the three types of information was required or authorised by or under law to avoid breach of s 101. The applicants submit that as the AFACT Notices put the respondent on notice that infringements were occurring, and as the respondent had the power to prevent those infringements, the respondent must at least have been authorised by s 280 to use the three types of information to take reasonable steps to prevent copyright infringement occurring.

535 Such submission is circular and rather 'puts the cart before the horse'. To make a finding of copyright authorisation complex issues must be resolved which require careful deliberation: it is not a matter that permits of straightforward resolution. The law of authorisation is not so simple as the applicants suggest. As already extracted from *Nationwide News* at 424, '*[k]nowledge that a breach of copyright is likely to occur does not necessarily amount to authorisation, even if the person having that knowledge could take steps to prevent the infringement*'. Indeed, even the AFACT Notices acknowledged the inherent uncertainty of the law of authorisation when they stated:

> The failure to take any action to prevent infringements from occurring, in circumstances where iiNet knows that infringements of copyright are being committed by its customers, or would have reason to suspect that infringements are occurring from the volume and type of the activity involved, **may** constitute authorisation of copyright infringement by iiNet. [emphasis added]

536 The Court has found that copyright authorisation is not made out in present circumstances. Consequently, use of the three types of information cannot have been required or authorised under the law merely by force of s 101.

537 The applicants alternatively submit that s 116AH(1) of the Copyright Act (part of the safe harbour provisions) authorise the disclosure of the information falling within s 276 of the

Telco Act. The applicants submit that as a requirement of those provisions is a 'repeat infringer policy', s 280 must authorise the use of the three types of information to implement that policy.

538 The safe harbour provisions may well authorise (they cannot '*require*', given their voluntary nature: see [589] below) the use of the three types of information. However, as will become apparent from the Court's discussion in Part F of this judgment, there is significant latitude given to a CSP to create its own repeat infringer policy. The respondent's repeat infringer policy provided that termination of subscriber accounts would not occur until such time as a Court ordered termination of a subscriber account, a person had been found by a Court to have infringed or had admitted infringement. None of these scenarios necessitate the use of any of the information absent a court order for such information's production. Therefore, s 280 cannot have authorised the information to be used because the respondent would not have been using that information for the purposes of complying with the safe harbour provisions. That is not to say that other CSPs with different repeat infringer policies would not be authorised under s 280 to use information of the kind discussed: the policies of each CSP would require their own interpretation.

539 Consequently s 280 cannot operate as an exception to the prohibition in relation to any of the three types of information.

Operation of s 290

540 The applicants further rely upon s 290 of the Telco Act which provides:

> **Implicit consent of sender and recipient of communication**
>
> Section 276 does not prohibit a disclosure or use by a person if:
>
> (a) the information or document relates to the contents or substance of a communication made by another person; and
>
> (b) having regard to all the relevant circumstances, it might reasonably be expected that the sender and the recipient of the communication would have consented to the disclosure or use, if they had been aware of the disclosure or use.

541 It is to be noted that s 290 is phrased in more limited terms to the previous two exceptions in that it only applies if '*the information or document relates to the contents or substance of a communication made by another person*'. Such phrase is more specific than

ss 279 and 280, suggesting that s 290 will only operate as an exception to information or a document which would fall under s 276(1)(a)(i) or (ii). Consequently, as the rumba information only falls under s 276(1)(a)(iv), that is, the information does not relate to a communication, s 290 could not operate as an exception allowing the use of that information, and it therefore cannot operate as a relevant exception in the present circumstances, because all three types of information must be used.

542 In relation to the score or AFACT information, there is no factual basis upon which it can be said that an iiNet user who has been infringing copyright might be said to have consented to the use of either the score or AFACT information were they to be made aware of that use. Accordingly, the Court does not consider that the circumstances permit the Court to find any basis that implicit consent exists even in relation to the information which could be excepted from s 276 by s 290.

Operation of s 289

543 Section 289 provides:

> **Knowledge or consent of person concerned**
>
> Division 2 does not prohibit a disclosure or use by a person of information or a document if:
>
> (a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and
>
> (b) the other person:
>
> (i) is reasonably likely to have been aware or made aware that information or a document of that kind is usually disclosed, or used, as the case requires, in the circumstances concerned; or
>
> (ii) has consented to the disclosure, or use, as the case requires, in the circumstances concerned.

544 It is to be noted that, similarly with s 290, s 289 is drafted more narrowly that ss 279 and 280. It only applies if '*the information or document relates to the affairs or personal particulars…of another person*'. Such section appears to have been drafted with similar wording to s 276(1)(a)(iv), to the exclusion of other types of information. However, it must be remembered that one type of information may satisfy the description of information of the type referred to in s 276(1)(a)(iv) *as well as* (i), (ii) and/or (iii). As already found, both the score and AFACT information is information of the type mentioned in s 276(1)(a)(i), (iii) *and*

(iv). The Court does not understand s 289 to apply to information which satisfies s 276(1)(a)(iv) only, and not other subsections. That is, the Court believes that s 289 will only apply to information if it meets the description of s 276(1)(a)(iv), but it will also apply to information which meets that description as well as others in s 276(1)(a)(i)-(iii).

545 As already discussed, all types of information (AFACT, score and rumba information) relate to s 276(1)(a)(iv), and, consequently, s 289 can operate as an exception to the prohibition on the use of all this information. That is, all the relevant information falls under s 289(a). The Court will now turn to s 289(b).

546 Turning first to s 289(b)(i), such section requires that the '*other person*', namely the subscriber, is '*reasonably likely*' to have been aware, or made aware, that the information or document '*of that kind*' is usually disclosed or used '*in the circumstances concerned*'. It cannot be suggested that any subscriber would be aware or be made aware, even by the CRA, that any information would be used against that person's contractual interests on the basis of the AFACT Notices. No circumstances are referred to in the CRA which could justify the use of any of the information on the basis referred to in s 289(b)(i).

547 Turning second to s 289(b)(ii), one of the obligations of a subscriber under the CRA is to '*comply with all laws and reasonable directions*' by the respondent (see clause 4.1). Clause 4.2 prohibits the use or attempted use of the respondent's services to infringe another person's rights or for illegal purposes. Clauses 14.2 and 14.4 authorise the respondent to cancel, suspend or restrict the service if it reasonably suspects illegal conduct by the subscriber.

548 Clause 12.3 of the respondent's CRA provides:

> We may collect, use and disclose Personal Information about you for the purposes of:

549 Nine purposes are then listed in clause 12.3 where the power to use and disclose Personal Information is permissible by the respondent, including:

> (c) providing the services you require from us and iiNet Related Entities;
>
> (d) administering and managing those services including billing, account management and debt collection;

550 The term 'Personal Information' is defined in clause 21.1 of the CRA as follows:

> **Personal Information** means information or opinion about you from which your identity is apparent or can reasonably be ascertained and includes your name, current and previous addresses, service number, date of birth, email address, bank account or credit card details, occupation, driver's licence number and your Credit Information and Credit Rating.

551 The words '*those services*' in clause 12.3(d) is clearly a reference to the service referred to in 12.3(c). The specific nature of the description of the services limits the occasions for the use of that information to that which is essentially for the administration of the CRA. The Court considers that as the respondent has (a) prohibited copyright infringing conduct pursuant to its CRA and (b) granted itself the right to cancel, suspend or restrict the use of the internet to subscribers who do infringe copyright, acting to further this end is relevantly part of administering and managing the respondent's services and the CRA.

552 Clause 12.3(d) creates a broad use for Personal Information for administering and managing the respondent's services, with the specific examples listed expressly not limiting the broader purpose because of the use of the word '*including*'. The Court rejects the respondent's argument that a broad reading of this subclause would render the other nine enumerated subclauses in 12.3 unnecessary. Clause 12.3(d) is purposely drafted as a wide subclause, but not so wide as to make the other subclauses redundant. For example, clause 12.3(a) states that Personal Information can be used for '*verifying your identity*', clearly not administering or managing those services, and clause 12.3(b) '*assisting you to subscribe to our services and the services of iiNet Related Entities*' would also not be eclipsed by a broad reading of clause 12.3(d). The respondent's submission does not stand up to a plain reading of the other subclauses.

553 The Court also rejects the argument of the respondent that acting on the AFACT Notices would not be account management. As stated, the relevant action here is enforcement of the CRA. Such action may be to the benefit of a third party, but that does not mean that the relevant characterisation of the action is purely in regards to that benefit. In making such finding, the Court repeats that the respondent's right to act under the CRA was not an obligation to act: however, if it chose to so act, it had the right to use the information by virtue of the CRA.

554 Consequently, pursuant to effect of clauses 4.1, 4.2, 14.2, 14.4 and 12.3(d), the respondent was given the right, by its subscriber's consent, to use all the relevant types of information. This satisfies s 279(a) and (b)(ii) which operates as an exception to non-disclosure mandated by s 276 of the Telco Act.

Conclusion

555 The Court concludes that disclosure or use of the AFACT information, score information or rumba information, which would otherwise be prohibited by s 276, may be disclosed or used due to the exceptions found in ss 289 and 279 of the Telco Act. Therefore, the Court finds that the Telco Act defence in and of itself did not mean that warning, termination or suspension of subscriber accounts based on the information found in the AFACT Notices was not relevant power to prevent infringement, pursuant to s 101(1A)(a) of the Copyright Act, or not a reasonable step, pursuant to s 101(1A)(c). However, this does not change the Court's view that, for all the reasons outlined in Part E1, authorisation is not made out in the present circumstances.

PART E3: SECTION 112E OF THE COPYRIGHT ACT

556 As the Court has found on conventional principles of copyright authorisation that the respondent has not authorised the infringements of the iiNet users, the Court need not deal with s 112E of the Copyright Act. However, the provision was the subject of extensive submission, and thus the Court considers that it should make findings in relation to the provision.

Section 112E

557 The *Copyright Amendment (Digital Agenda) Act* inserted s 112E into the Copyright Act. Section 112E provides that:

> 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 an audio-visual item merely because another person uses the facilities so provided to do something the right to do which is included in the copyright.

Pursuant to s 100A the identified films, as cinematograph films, are 'audio-visual' items for the purposes of s 112E.

558 The Explanatory Memorandum to the *Copyright Amendment (Digital Agenda) Bill* states at [138] that s 112E:

> …has the effect of expressly limiting the liability of carriers and carriage service providers for authorisations of copyright infringement on their networks. The section provides that carriers and carriage service providers will not be taken to have authorised an infringement of copyright in a film, sound recording, television broadcast or sound broadcast merely because they provide the facilities by which that material is communicated to the public. The reference to "facilities" is intended to include physical facilities and the use of cellular, satellite and other technologies.

The Bill was subsequently amended to remove the need for facilities to be physical facilities. A Supplementary Explanatory Memorandum provided at [64] in relation to the amended s 112E (that is, s 112E in its current form and extracted at [557] above):

> …clause s 112E has the effect of expressly limiting the authorisation liability of persons who provide facilities for the making of, or facilitating the making of, communications. The clause provides that such persons are not taken to have authorised the infringement of copyright in an audio-visual item merely because another person has used the facilities to engage in copyright infringement.

559 During the Second Reading Speech of the Bill, the Honourable Daryl Williams MP said:

> The provisions of the bill limit and clarify the liability of carriers and Internet service providers in relation to both direct and authorisation liability. The amendments also overcome the 1997 High Court decision of APRA v. Telstra [sic – the High Court decision was *Telstra v APRA*] in which Telstra, as a carrier, was held to be liable for the playing of music-on-hold by its subscribers to their clients, even though Telstra exercised no control in determining the content of the music played.
>
> …
>
> The reforms provide that a carrier or Internet service provider will not be taken to have authorised an infringement of copyright merely through the provision of facilities on which the infringement occurs.

Judicial Authority

Kazaa

560 In *Kazaa*, Wilcox J adopted a narrow interpretation of s 112E, stating (at [396]) that:

> [i]f the most that can be said against Sharman is that it has provided the facilities used by another person to infringe copyright, Sharman is not to be taken to have authorised the infringement. So understood, s 112E operates as a legislative reversal of the High Court's decision in [*Telstra v APRA*].

His Honour then said (at [399]):

> A statutory provision to the effect that a person is not taken to have authorised an infringement merely because another person does a particular thing leaves open the possibility that, for other reasons, the first person may be taken to have authorised the infringement. Such a provision does not confer general immunity against a finding of authorisation. Consequently, s 112E does not preclude the possibility that a person who falls within the section may be held, for other reasons, to be an authoriser. Whether or not the person should be so held is to be determined, in the present context, by reference to s 101 of the Act.

His Honour then went on to consider authorisation and s 112E in relation to Sharman. He stated (at [401]) that:

> Sharman is not held to have authorised copyright infringement by Kazaa users merely because it provides the facilities they use in order to infringe the applicants' copyright. Something more is required. In evaluating the "something more", regard must be paid to the factors listed in s 101(1A) of the Act…

561 His Honour then considered, with reference to s 101(1A) criteria, together with other factors, whether Sharman had authorised the infringement of copyright. His Honour found that Sharman had authorised because it had provided the facilities for file-sharing ([403]); had a financial interest in there being increasing amounts of file-sharing ([404]); had positively encouraged infringement ([405]); knew of the infringements ([406]); and had the power to prevent the infringements occurring ([411]). Following this discussion, his Honour stated (at [418]) in relation to s 112E:

> I accept that parliament intended to "protect the messenger", although only to the extent indicated by the Act; notably s 112E. However, on my findings, Sharman is and was more than a "messenger".

Equally, his Honour found (at [468]) that:

> On the basis that Altnet and Sharman jointly provide Kazaa, Altnet is a person to whom s 112E of the Act applies. Altnet "provides facilities", in conjunction with Sharman, within the meaning of that section. However, on the stated basis, Altnet does more than provide facilities for making, or facilitating the making of a communication. It is involved in Sharman's additional activities.

562 Unfortunately his Honour never elucidated precisely what it was that made Sharman '*more than a messenger*' aside from the general factors that his Honour considered were relevant to his finding that Sharman had authorised copyright infringement. Thus although it is clear that, pursuant to his Honour's reasons, '*something more*' than mere provision of facilities can cause s 112E to lose its effect, it is not clear from his reasons what that

'*something more*' specifically was in that proceeding, aside from general authorisation considerations.

Cooper 150 FCR 1

563 Tamberlin J dealt with the question whether s 112E applied to Mr Cooper or Comcen, the ISP in those proceedings. His Honour noted (at [98]) that s 112E only applies to protect against a finding of copyright authorisation, not primary infringement. His Honour then went on to find, in relation to Mr Cooper, that there were two factors that took Mr Cooper outside the protection of s 112E. They were (at [99]):

> …because Cooper has offered encouragement to users to download offending material, as evidenced by the numerous references to downloading material on the website, and has specifically structured and arranged the website so as to facilitate this downloading.

564 In relation to Comcen, Tamberlin J noted what would appear to be three factors which took the ISP outside of the protection of s 112E. First (at [126]):

> Accordingly, within the meaning of s 112E, it could not be said that they were doing no more than "merely" hosting the website involved in the present circumstances. Where a host is on notice of an irregularity, deliberately elects not to investigate the operation and contents of a site and turns a blind eye to such indications, even having regard to the possible indication afforded by the title of the website, then, in my view, there are additional factors called into play beyond merely hosting the website.

As an aside, it must be remembered that the '*irregularity*' referred to above existed in relation to the very activities to which Comcen was a party. In the present circumstances any '*irregularity*' was not observed by the respondent and was not brought about because of its actions. The second and third factors were (at [131]):

> The word "merely" must be given its full force and effect. The second to fifth respondents have assumed an active role by agreeing to host the website and assisting with the operation of the website, which are necessarily steps to effectively trigger the downloading of the copyright material. The reciprocal consideration passing between them, namely, the free hosting in return for the display of the Com-Cen logo on the website, is an additional matter which takes the situation beyond the protection afforded by s 112E.

Cooper 156 FCR 380

565 On appeal, both Branson and Kenny JJ upheld Tamberlin J's finding. Branson J noted in her judgment that s 112E '*qualifies the operation of s 101(1A)*' (at [19]). Her Honour

found at [56] that the effect of s 112E was that '*E-Talk is not to be taken to have authorised any infringement of copyright in a sound recording just because internet users used Mr Cooper's website to download music files of sound recordings…*'. However, her Honour found at [58]-[60] that Comcen had done more than this, given that Comcen was an ISP; had hosted Mr Cooper's website; '*was aware of the high level of usage of Mr Cooper's website and the copyright problems*'; had provided Mr Cooper with free web hosting in exchange for Mr Cooper placing the Comcen logo and hyperlink on his website; and had taken no steps to prevent the infringement.

566 Kenny J approved at [168] the comments of Wilcox J in *Kazaa*, as extracted above, where his Honour noted that s 112E was intended to reverse the effect of *Telstra v APRA*; that there may be other reasons than the provision of facilities which takes a person outside of the protection of s 112E ([168]); and that those other reasons depend on factors pursuant to s 101(1A) and other matters ([168]). In relation to Mr Cooper, Kenny J found (at [169]):

> …the website [www.mp3s4free.net] constituted an invitation by Mr Cooper to internet users to use the hyperlinks that it provided and to add new links, in order that sound recordings could be downloaded from remote computers and thereby copied. Having regard to the matters already mentioned with respect to Mr Cooper, it cannot be said that he did no more than provide the facilities that were used to infringe the Record Companies' copyright.

Similarly to the extract from Wilcox J in *Kazaa*, Kenny J did not precisely characterise what it was that took Mr Cooper out of the protection of s 112E. Kenny J was more specific in relation to Comcen (at [170]):

> E-Talk, and, through E-Talk, Mr Bal, derived a commercial advantage from the website operated by Mr Cooper that was over and above payment for hosting services. Mr Bal, and through him, E-Talk, knew about the website and the infringements of copyright that were likely to be committed through its operation. In that knowledge, neither took reasonable steps to prevent the infringements.

567 The High Court refused an application for special leave to appeal by Comcen and Mr Bal: *E-Talk Communications Pty Ltd & Anor v Universal Music Pty Ltd & Ors* [2007] HCATrans 313 ('*E-Talk*'). Gummow J refused leave saying: '*[h]aving regard to the factual findings made in this case, both at first instance and confirmed in the Full Court, there are insufficient prospects of success, on the issues of law which the applicants propound, to warrant a grant of special leave*'.

The Court's interpretation of s 112E

568 Before discussing the Court's view of s 112E, a discrete issue requires mention. As stated, Wilcox and Kenny JJ expressly found that s 112E operated as a reversal of *Telstra v APRA*. The difficulty with that view of s 112E is that s 112E only operates to prevent a finding of copyright authorisation, not a finding of primary infringement. *Telstra v APRA* involved a finding that Telstra had infringed APRA's copyright directly, pursuant to the now repealed s 26 of the Copyright Act and therefore that Telstra was a primary infringer. Consequently, if s 112E operates as a legislative reversal of *Telstra v APRA*, it operates as a very particular kind of reversal, given that it does nothing to protect against a finding that an ISP, for example, directly infringed copyright, which was the very finding that was made against Telstra in *Telstra v APRA*.

569 An analysis of the extrinsic material, particularly the Advisory Report on the *Copyright Amendment (Digital Agenda) Bill 1999* at 99-100 suggests that it was in fact the new communication right in s 86(c) and s 10 of the Copyright Act and the amendment to s 22(5) and s 22(6) of the Copyright Act which was intended to reverse the effect of *Telstra v APRA*, not s 112E. Such report states:

> Telstra argued that proposed s.22(6) correctly implements the principle necessary to avoid liability such as that imposed by the music on hold case. The Law Council of Australia made a submission to like effect. [footnotes omitted]

This was acknowledged by Tamberlin J in *Cooper* 150 FCR 1 at [70]. This suggests that Wilcox and Kenny JJ were incorrect in their finding that s 112E operates as a legislative reversal of *Telstra v APRA*.

570 In the present proceeding, the applicants submit that, pursuant to *Cooper* (first instance and appeal) and *Kazaa* discussed above, '*as soon as any factual element is present that bears upon the question of authorisation, the provisions of s 112E are of no consequence*'. This would appear to generally accord with the interpretation of the section pursuant to judicial authority binding on this Court. As stated, Wilcox J, without specification, appeared to find that the factors which led him to conclude that authorisation was made out led him to find that s 112E did not assist Sharman. Tamberlin J, at first instance, and Branson and Kenny JJ, on appeal, appeared to focus on the level of knowledge of the ISP of Mr Cooper's website which facilitated the infringement as well as the

commercial relationship between Comcen and Mr Cooper which went beyond the usual hosting arrangement between an ISP and a subscriber as being the factors which took the ISP outside the protection of s 112E.

571 The respondent submits that such approach deprives s 112E of its effect, given that any factor which would go to authorisation takes a person out of the protection of s 112E, thereby meaning that s 112E, which is meant to protect against a finding of authorisation, automatically falls away upon the finding of authorisation. The submissions have some merit, though they are not correct. The approach does not deprive s 112E of any effect, but it does give it a minimal effect.

572 For example, s 112E may have some effect vis-à-vis the role of Telstra in the present circumstances. The evidence suggests that, at least with ADSL connections, a necessary physical facility for the connection of iiNet users to the internet is the copper phone lines which are owned by Telstra: see [53] above. Consequently, Telstra's physical facilities are a necessary precondition to any infringements of the iiNet users. Section 112E would appear to have some work in the present circumstances to protect Telstra, but only in the circumstance that Telstra's mere provision of copper wires could actually constitute copyright authorisation. Another example suggested by Mr Nicholas SC (as he then was) in the special leave application before the High Court in *E-talk* was:

> …in circumstances where an Internet service provider was making available facilities which were being used for the purpose of facilitating communications which, unbeknown to the service provider, constituted infringing communication, then plainly we would say section 112E would have some work to do.

573 However, it would appear to be highly unlikely that in either of the above examples, Telstra or the hypothetical ISP could be found to have authorised infringement. In short, it would appear that s 112E provides protection when it is not needed. Yet, in making such statement the Court is mindful of the Full Federal Court authority (see Branson J at [32] in *Cooper* 156 FCR 380) which states s 112E '*…presupposes that a person who merely provides facilities for making a communication might, absent the section, be taken to have authorised an infringement of copyright in an audio-visual item effected by the use of the facility*'.

574 In summary, the authorities appear to leave little room for s 112E to have meaningful operation. It will not protect a person from authorisation when there is a factor found to exist

which entitles a finding of authorisation. Therefore, such finding renders s 112E inapplicable when authorisation is found, or, as the applicants submitted, '*[i]nevitably, when a finding of authorisation is made against a provider of facilities, s 112E will not assist, as in all of the circumstances that person is doing more than (or in addition to) providing services*'. Therefore, the only circumstance when s 112E could have an effect is when the person merely provides the facilities for the making of the infringement *and does nothing more*. However, as stated, it is highly unlikely that there will be any circumstance where the mere provision of the facilities would constitute authorisation, especially given that '*the word "authorize" connotes a mental element [such that] it could not be inferred that a person had, by mere inactivity, authorized something to be done if he neither knew, nor had reason to suspect that the act might be done*': per Gibbs J in *Moorhouse* at 12. Consequently, it appears that s 112E purports to provide protection when no occasion could arise to require that protection. These issues were canvassed before the High Court in the special leave application in *E-Talk* but the High Court saw fit not to grant special leave.

575 The Court, while sympathetic to the problems highlighted by the respondent in regard to the judicial interpretation of s 112E, is prevented from interpreting s 112E differently. It is bound to follow the Full Court's interpretation.

Can the respondent take advantage of s 112E?

576 In the present circumstance, the applicants submit that there are four factors relevant to a finding of authorisation which relevantly take the respondent outside of the protection of s 112E. The first is the respondent's knowledge of infringements; the second the respondent's contractual relationship with its subscribers; the third the respondent's positive encouragement of infringement; and the fourth the respondent's commercial interests. As found at [486] the Court has not found that the respondent positively encouraged infringement. As regards to the respondent's financial interests, as stated at [238], they were remote from the infringements that occurred. The Court does not consider that the presence of a contractual relationship is a relevant factor, given that s 112E was drafted with CSPs in mind (they are specifically mentioned in the text of s 112E), and it is to be expected that CSPs would have a contractual relationship with their subscribers.

577 Therefore, the only relevant factor identified by the applicants which could be the '*something more*' (as per Wilcox J) which would take the respondent out of s 112E protection is the respondent's knowledge of the infringements which were committed by the iiNet users. Knowledge of infringements was found to be a relevant factor in *Kazaa* (by inference, given that it was a relevant factor to the finding of authorisation in that case), *Cooper* 150 FCR 1 at [126] and *Cooper* 156 FCR 380 at [58] per Branson J and [170] per Kenny J.

578 The Court has found at [471] that the respondent had, at some point, knowledge sufficient to act. Such finding has not led the Court to conclude that the respondent authorised copyright infringement. However, on the judicial authority as discussed, it appears that finding has the result that s 112E protection is not available. Based upon the above authorities, as long as the alleged authoriser has knowledge of infringements, s 112E will cease to operate. Consequently, the Court must find that s 112E would not have operated to protect the respondent from a finding of authorisation.

Conclusion

579 As the respondent had knowledge of the infringements which were occurring on its facilities and as such factor is relevant to a finding of authorisation (though, in this circumstance has not led to such finding), according to authority binding upon this Court, s 112E ceased to have operation. However, such finding is an irrelevancy given that the Court has already found that, regardless of s 112E, the respondent did not authorise infringement.

PART F: SAFE HARBOUR PROVISIONS

580 The finding of the Court that the respondent did not authorise the copyright infringing acts of the iiNet users renders it unnecessary for the respondent to rely upon the safe harbour provisions found in Division 2AA of Part V of the Copyright Act. However, as with the discussion in regards to s 112E, the Court finds that, given the extensive argument before the Court on the issue, the paucity of judicial consideration of the provisions (*Cooper* 150 FCR 1 only shortly discussed the provisions at [103]-[109]), and the relevance of the provisions for the internet industry more broadly, there is value in the Court making its findings in regards to the safe harbour provisions.

581 The safe harbour provisions were introduced into the Copyright Act by means of the *US Free Trade Implementation Act 2004* (Cth) and the *Copyright Legislation Amendment Act 2004* (Cth). There were also ancillary amendments made to the *Copyright Regulations 1969* (Cth) ('the Regulations') by means of the *Copyright Amendment Regulations 2004 (No. 1)* (Cth). As the mention of the US Free-Trade Agreement suggests, the provisions in the Copyright Act had their origin in US law, specifically s 512 of Title 17 of the *United States Code* (US) ('17 USC § 512') which had its origin in s 202 of the DMCA. As will be made clear, while there are some differences between the United States and Australian 'safe harbo(u)rs', US authorities can provide significant assistance in the interpretation of the Copyright Act safe harbour provisions.

582 The Australian provisions, unlike the US provisions which are broader in their operation (see § 512(k)), only provide protection for CSPs. Carriage Service Provider is defined in s 10 of the Copyright Act in the same terms as in the Telco Act, namely:

> **87 Carriage service providers**
>
> *Basic definition*
>
> (1) For the purposes of this Act, if a person supplies, or proposes to supply, a listed carriage service to the public using:
>
> (a) a network unit owned by one or more carriers; or
>
> (b) a network unit in relation to which a nominated carrier declaration is in force;
>
> the person is a ***carriage service provider***.

As mentioned, there is agreement between the parties that the respondent is a CSP. The Australian provisions, like the US provisions, concern four different and mutually distinct types of activity (though the one CSP might undertake more than one kind of activity).

583 The first, category A, which is relevant for these proceedings, occurs when CSPs '*provid[e] facilities or services for transmitting, routing or providing connections for copyright material, or the intermediate and transient storage of copyright material in the course of transmission, routing or providing connections*' (s 116AC). This category is often referred to as 'transmission' activities. The second, category B (s 116AD), refers to 'caching' activities, the third, category C (s 116AE), 'hosting' activities and finally category D (s 116AF), is 'information location' activities. While the other categories may be referred to

in the following discussion, there is no dispute that the relevant activity for the present proceeding is category A activities. The Explanatory Memorandum to the *US Free Trade Implementation Bill 2004* ('safe harbour EM') at 160 makes clear that the qualification for one category by a CSP does not affect the determination of whether that CSP is, or is not, capable of qualifying for any other category.

584 If the CSP satisfies the conditions attached to a particular category (discussed below) the remedies available to a copyright owner for the copyright infringement (whether primary or authorising) against the CSP are found in s 116AG. Subsection (2) of s 116AG places a bar on the Court granting any damages, additional damages, account of profits or other monetary relief against a CSP. Subsection (3), which refers to category A activities (categories B-D are discussed in subsection (4)), limits the remedies a Court can make to '*an order requiring the carriage service provider to take reasonable steps to disable access to an online location outside Australia*' and/or '*an order requiring the carriage service provider to terminate a specified account*'. In deciding whether to make such order, the Court must have regard to (s 116AG(5)):

> (a) the harm that has been caused to the owner or exclusive licensee of the copyright; and
>
> (b) the burden that the making of the order will place on the carriage service provider; and
>
> (c) the technical feasibility of complying with the order; and
>
> (d) the effectiveness of the order; and
>
> (e) whether some other comparably effective order would be less burdensome.
>
> The court may have regard to other matters it considers relevant.

Interaction between the safe harbour provisions and copyright authorisation

585 Division 2AA of Part V is headed '*Limitation on remedies available against carriage service providers*'. Section 116AA states:

> (1) The purpose of this Division is to limit the remedies that are available against carriage service providers for infringements of copyright that relate to the carrying out of certain online activities by carriage service providers. A carriage service provider must satisfy certain conditions to take advantage of the limitations.
>
> (2) This Division does not limit the operation of provisions of this Act outside this Division in relation to determining whether copyright has been infringed.

586 As both subsections make clear, Division 2AA only becomes relevant *after* a finding that a CSP is liable for copyright infringement. It can only logically be thus. The purpose of the provision is to limit *remedies* available against a party and a remedy only becomes relevant if liability is established.

587 The safe harbour EM states (at 157) in relation to s 116AA(2):

> While actions taken by a carriage service provider in relation to the condition set out in this Division may have some relevance to whether or not copyright infringement has occurred, the Division does not affect the way provisions in the Act in relation to the determination of liability should be interpreted or limit the application of the exceptions in the Act. Further, the failure of a carriage service provider to qualify for any limitation on remedies in this Division does not make the service provider liable for copyright infringement. A copyright owner must still establish that a carriage service provider has infringed copyright under the Act.

588 Further, s 116AH(2) states:

> Nothing in the conditions is to be taken to require a carriage service provider to monitor its service or to seek facts to indicate infringing activity except to the extent required by a standard technical measure mentioned in condition 2 in table item 1 in the table in subsection (1).

589 The Court considers that the combined effect of such provisions and the voluntary nature of any industry code (reg 20B of the Regulations) have two consequences. First, that compliance with safe harbour requirements may be evidence that can be relevant to show that a CSP ought not be rendered liable for copyright infringement. Therefore, should a CSP implement a scheme in relation to category A activities which complies with condition 1 of item 1 of s 116AH(1), that may be evidence in favour of a finding that the CSP did not authorise the infringement of copyright or infringe copyright directly. Second, the Court considers that the reverse is not true. That is, failure to comply with the requirements of the safe harbour provisions *cannot* be relevant and is not evidence that goes to a finding that a CSP is liable for copyright infringement, since this would defeat the voluntary nature of the safe harbour provisions. Parliament has implemented a voluntary inducement, which, if not taken up, cannot, per se, be used as evidence that the CSP has authorised infringement. In other words, if a CSP does not implement such a scheme, that is a wholly irrelevant consideration for the purposes of deciding whether a CSP authorised infringement. Failure to comply merely has the consequence that the CSP cannot take advantage of Division 2AA

should they be found to have authorised. For this reason the applicants were in error in making the submissions discussed at [431]-[432] above.

What is a repeat infringer policy?

590 In order for a CSP to take advantage of the safe harbour provisions, it must comply with conditions found in Subdivision D of Division 2AA: see s 116AG(1). CSPs must comply with conditions 1 and 2 of item 1 in s 116AH(1) in relation to categories A-D. They are:

> 1. The carriage service provider must adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers ['repeat infringer policy'].
>
> 2. If there is a relevant industry code in force-the carriage service provider must comply with the relevant provisions of that code relating to accommodating and not interfering with standard technical measures used to protect and identify copyright material.

CSPs must then comply with further conditions, specific to each category. Category A requires compliance with a further two conditions in item 2 of s 116AH(1):

> 1. Any transmission of copyright material in carrying out this activity must be initiated by or at the direction of a person other than the carriage service provider.
>
> 2. The carriage service provider must not make substantive modifications to copyright material transmitted. This does not apply to modifications made as part of a technical process.

591 Section 116AI provides:

> If a carriage service provider, in an action relating to this Division, points to evidence, as prescribed, that suggests that the carriage service provider has complied with a condition, the court must presume, in the absence of evidence to the contrary, that the carriage service provider has complied with the condition.

Given such provision and the evidence presented in these proceedings, the Court finds that conditions 1 and 2 of item 2 were complied with by the respondent. Therefore, the relevant dispute is in regards to condition 1 of item 1, specifically whether the respondent had a policy '*that provides for termination, in appropriate circumstances, of the accounts of repeat infringers*' and, if it does, whether it '*reasonably implement[ed]*' such a policy.

592 According to the safe harbour EM at 161, this repeat infringer policy '*is to be determined by the carriage service provider*'. The repeat infringer policy required is phrased

slightly differently in the safe harbour EM to that in the Copyright Act itself, the former stating that it must be a policy for '*terminating in appropriate circumstances the accounts of users who are repeat copyright infringers*'.

593 It is impossible to fail to notice the complete vacuum of legislative guidance in relation to any category A requirements when compared to the highly prescriptive requirements in relation to categories B-D found in s 116AH(1) and the Regulations. Neither the legislation, the Regulations nor extrinsic materials provide any guidance to the Court as to what the '*appropriate circumstances*' for termination are, what '*repeat infringement*' means or what the '*accounts of repeat infringers*' means. The assumption must be that Parliament left latitude with the CSP to determine the policy, and left the meaning of those words to be determined by the courts.

594 To add to the confusion, condition 1 of item 1 applies to all categories of activities, even though a 'repeat infringer' in relation to category A is likely to be different to a 'repeat infringer' in relation to category C (hosting), for example. This is likely to be important, given that the termination must occur only in '*appropriate circumstances*'. For example, it could be argued that given that the legislation and the Regulations in relation to category C (hosting) are highly prescriptive and that that type of activity allows for a CSP to actually access and view the material alleged to be infringing, that would have the consequence that it would be reasonable for the repeat infringer policy in relation to that category to provide for quicker termination of internet users alleged to be repeat infringers than in relation to category A, where, due to the transitory nature of the transmission, a CSP cannot independently verify the infringing nature of the transmission. Presumably, given that condition 1 of item 1 is said to apply to all categories, implementing an appropriate repeat infringer policy in relation to one category will not necessarily suffice for compliance with another category.

US precedent on safe harbor provisions

595 Given this vacuum of legislative or judicial guidance, the Court turns to US precedent. The US safe harbor provisions create very similar requirements to the Copyright Act safe harbour provisions in relation to the requirements of categories A-D (there defined as § 512(a)-(d)), and, as already discussed, the Australian provisions were modelled on the US provisions.

Further, the US safe harbor provisions create a virtually identical requirement for a service provider to adopt a repeat infringer policy to the Copyright Act (at § 512(i)(1)):

> The limitations on liability established by this section [§ 512] shall apply to a service provider only if the service provider –
>
> (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers…

The section '*and informs subscribers…or network of*' is omitted in the Copyright Act (an issue discussed below). However, in all other relevant respects, s 116AH(1) item 1 condition 1 and § 512(i)(1)(A) are the same. However, given the discussion above at [594], it is important to keep in mind that not all US decisions deal with category A activities, and thus the requirements of a repeat infringer policy in regards to another category may not be appropriate to rely upon for interpretation of category A.

596 A number of US cases have dealt with § 512(i)(1)(A). US decisions appear to divide the requirements of § 512(i)(1)(A) into three parts: see, for example, *Corbis Corporation v Amazon.com, Inc* 351 FSupp2d 1090 (WD Wash 2004) ('*Corbis*') at 1100:

> A service provider must: 1) adopt a policy that provides for the termination of service access for repeat copyright infringers in appropriate circumstances; 2) inform users of the service policy; and 3) implement the policy in a reasonable manner.

The second requirement comes from the wording of the US provision which, as mentioned in the paragraph above, does not precisely mirror s 116AH(1) condition 1 of item 1. There is no statutory requirement for the notification of such a policy to a CSP's subscribers pursuant to condition 1 of item 1 of s 116AH(1) of the Copyright Act.

REQUIREMENTS OF THE POLICY

597 A key authority in relation to the first requirement, the creation of a policy, is *In Re: Aimster Copyright Litigation* 252 FSupp2d 634 (ND Ill 2002) ('*In re Aimster* 252 FSupp2d 634') (first instance); and 334 F3d 643 (7th Cir 2003) (appeal). In the first instance decision Aspen CJ found (at 658-659) that Aimster had a repeat infringer policy due to two factors. The first factor was a notice on the Aimster website which: (a) stated that Aimster '*respect[s] copyright law and expects our users to do the same*'; (b) outlined its procedure for the takedown of infringing material; and (c) stated that '*users who are found to repeatedly violate*

the copyrights of others may have their access to all services terminated'. The second factor was the provision of a form for copyright owners to notify Aimster of copyright material being infringed. This satisfied the requirement of a repeat infringer policy.

598 On appeal, Posner J, writing the opinion for the Appeal Court, affirming Aspen CJ, dealt with the issue rather more briefly. Posner J found (at 655):

> The common element of its safe harbors is that the service provider must do what it can reasonably be asked to do to prevent the use of its service by "repeat infringers". 17 U.S.C. § 512(i)(1)(A). Far from doing anything to discourage repeat infringers of the plaintiffs' copyrights, Aimster invited them to do so, showed them how they could do so with ease using its system, and by teaching its users how to encrypt their unlawful distribution of copyrighted materials disabled itself from doing anything to prevent infringement.

599 With the greatest respect to his Honour, § 512(i)(1)(A) does not accord with his Honour's encapsulation of that section. The section does not state that there is any broad duty for a service provider '*to do what it can reasonably be asked to do to prevent the use of its service by "repeat infringers"*'. It does not state positively that the service provider must '*discourage repeat infringers*'. It merely states that the service provider should have '*adopted and reasonably implemented, and inform[ed] subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers*' in order to take advantage of the US safe harbor.

600 With respect to his Honour, his reasoning appears to convert a provision designed to limit remedies where liability for copyright infringement is already established into a positive duty to prevent copyright infringement. The submissions of the applicants in these proceedings occasionally adopted the same philosophy. Section 512(i)(1)(A) does no such thing, nor does condition 1 of item 1 of s 116AH(1) of the Copyright Act. In short, the Court prefers the judgment of Aspen CJ to provide guidance in the interpretation of what a repeat infringement policy is for the purposes of s 116AH(1) item 1 condition 1 of the Copyright Act.

601 A further useful authority is *Corbis*. In that decision, Lasnik J, dealing with category C activities, found that Amazon had a repeat infringer policy. While Corbis, the plaintiff, had argued that Amazon's policies were '*too vague with regard to issues of copyright infringement…do not include the term "repeat infringer" and do not describe the methodology*

employed in determining which users will be terminated for repeated copyright violations' (at 1100), his Honour rejected such argument. He found (at 1101):

> The key term 'repeat infringer', is not defined and the subsection never elaborates on what circumstances merit terminating a repeat infringer's access. This open-ended language contrasts markedly with the specific requirements for infringement notices and take-down procedures…[t]he fact that Congress chose not to adopt such specific provisions when defining a user policy indicates its intent to leave the policy requirements, and the subsequent obligations of the service providers, loosely defined.

His Honour found at 1101:

> Given the complexities inherent in identifying and defining online copyright infringement, § 512(i) does not require a service provider to decide, ex ante, the specific types of conduct that will merit restricting access to its services…[however,] it is clear that a properly adopted infringement policy must convey to users that "those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others…know that there is a realistic threat of losing that access."

His Honour concluded at 1101 that Amazon's policies conveyed that message, given that it informed vendors in its Participation Agreement that those '*accused of copyright infringement are informed that repeated violations could result in "permanent suspension" from Amazon sites*'.

IMPLEMENTATION OF THE POLICY

602 *In re Aimster* 252 FSupp2d 634 is also a useful authority relating to the third requirement, namely the actual implementation of a repeat infringer policy. Aspen CJ found that while Aimster had a policy, it had not implemented it. His Honour found that as the encryption feature of Aimster rendered it impossible for Aimster or copyright owners to identify which Aimster users were transferring which files, Aimster had '*evicerat[ed] any hope that such a policy could ever be carried out*' (at 659). Consequently, Aimster's policy was a '*mirage*' and was not implemented: see 659.

603 In *Harlan Ellison v Steven Robertson* 357 F3d 1072 (9th Cir 2004) ('*Ellison* 357 F3d 1072'), Pregerson J found at 1080 that while AOL had a repeat infringer policy, it had failed to implement it because it did not have an effective notification procedure in place at the time the alleged infringements were taking place. The procedure was ineffectual because AOL had changed the email address that notifications of copyright infringement were to be sent to without providing notification to the US Copyright Office or on its website. It did not

implement a system whereby notifications sent to the old address were forwarded to the new address. This meant that '*AOL allowed notices of potential copyright infringement to fall into a vacuum and go unheeded; that fact is sufficient for a reasonable jury to conclude that AOL had not reasonably implemented its policy against repeat infringers*' (at 1080).

604 In the decision of *Perfect 10, Inc v Cybernet Ventures, Inc* 213 FSupp2d 1146 (CD Cal 2002) ('*Cybernet*') at 1177 Baird J found that '*appropriate circumstances*' to terminate repeat infringers would include, '*at a minimum, instances where a service provider is given sufficient evidence to create actual knowledge of blatant, repeat infringement by particular users, particularly infringement of a wilful and commercial nature*'.

605 Despite such finding, in the latter decision of *Corbis*, mentioned above, Lasnik J placed a high level of proof for such instances, stating at 1104-1105 that '*it requires, at a minimum, that a service provider who receives notice of a copyright violation be able to tell merely from looking at the user's activities, statements, or conduct that copyright infringement is occurring*'. His Honour found at 1105 that notices pursuant to category C activities were not the '*sine qua non of copyright liability*' and that '*notices alone do not make the user's activity blatant, or even conclusively determine that the user is an infringer*'. Therefore, although '*the notices have brought the listings to Amazon's attention, they did not, in themselves, provide evidence of blatant copyright infringement*': see 1105.

606 In the decision of *Perfect 10, Inc v CCBill LLC* 481 F3d 751 (9th Cir 2007), a matter concerned with category C activities, Smith J, after reflecting on the authorities, found (at 758) that '*a service provider "implements" a policy if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications…[t]he statute permits service providers to implement a variety of procedures…*'.

CONCLUSIONS

607 In general, the US authorities appear to approach the question whether a service provider has a repeat infringer policy and whether it has implemented that policy as a preliminary or 'threshold' question before addressing the question as to which category is satisfied by the activities in question, and whether the particular requirements of the specific

categories have been met: see, for example, *Harlan Ellison v Stephen Robertson* 189 FSupp2d 1051 (CD Cal 2002) and 357 F3d 1072; *Cybernet*; *In re Aimster* 252 FSupp2d 634; *Perfect 10, Inc* v *CCBill, LLC* 340 FSupp2d 1077 (CD Cal 2004) and 481 F3d 751; and *Corbis*. This reasoning probably results from the structure of 17 USC § 512 which phrases the repeat infringer policy as one of the '*Conditions for Eligibility*' of the US safe harbor provisions. In contrast, s 116AH(1) of the Copyright Act places the conditions to be complied with by CSPs in relation to all categories in the same table as the specific conditions for each category. For this reason, and the reasons discussed above at [594], the Court finds that it is more appropriate to consider whether a CSP has a repeat infringer policy directed to a particular category of activity (that is, A-D) rather than in the abstract.

608 The requirements of the repeat infringer policy itself appear to be minimal, with significant latitude granted to service providers to determine the policy. Under US law, the policy appears to require some kind of viewable notification of the policy to the service provider's users (though it must be remembered that this is in the context of the requirement that the service provider's users be informed of the policy, a requirement not present in condition 1 of item 1 in s 116AH(1)) and the service provider must have a mechanism for notifications to be provided to it alleging copyright infringement. The latter requirement would appear to be required at least for the purposes of notification and takedown procedures of categories B, C and D activities. The policy need not be prescriptive in terms of precisely those matters which will constitute repeat infringement and which will lead to termination.

609 As to implementation of that policy, the authorities, particularly *Ellison* 357 F3d 1072 and *In re Aimster* 252 FSupp2d 634 make clear that a service provider cannot take *positive* steps that, in effect, prevent a copyright owner from being able to provide to the CSP notifications of alleged copyright infringing activities. The service provider must have an operative notification system to receive notices from copyright owners and a procedure to act on notifications given. Finally, the service provider will not be found to have implemented that policy if it takes no action to terminate users when a notice enables a service provider to know that blatant copyright infringement is occurring '*merely from looking at the user's activities, statements, or conduct*': see *Corbis* at 1104-1105.

610 This Court adopts the abovementioned US authority. Given the similarity in the relevant statutory instruments and the dearth of Australian authority interpreting the safe harbour provisions, the Court considers that it is of immense assistance to consider those decisions of US Federal Courts where similar provisions have been interpreted. However, in adopting the authorities, the Court is mindful of those instances in which Australian and US copyright law differs.

Did the respondent have a repeat infringer policy?

611 The Court finds that the respondent had a repeat infringer policy. As the authorities outlined above suggest, the requirements of such policy are not extensive, given that the legislature saw fit to leave the form of the policy up to the particular CSP.

612 The Court finds evidence for the existence of the policy in two documents and Mr Malone's oral evidence. The first document is the copyright section of the respondent's website which states:

> New Copyright regulations came into play on 1st January 2005 as a result of the US Free Trade Agreement. The new regulations allow for Copyright owners to provide notice in accordance with the prescribed format set out in the "Copyright Act" to a service provider of any infringing material.
>
> A notice of copyright infringement in the prescribed format in accordance with the Copyright Act can be sent to: …
>
> [contact details provided]
>
> **NOTE:** The hosting or posting of copyright material using an iinet service constitutes a breach of iinet contractual obligation under the Customer relationship Agreement Sec 4.1 & Sec 4.2 Customer relationship Agreement. Such a breach of contract may result in the suspension or termination of service without notice to the subscriber.

613 The second document is the CRA which was changed in 2005 to provide for the ability for the respondent to terminate subscriber accounts due to copyright infringement. Mr Malone pointed to these two documents in his cross-examination as evidence of the existence of the policy:

> And you agree with me that one can spend the rest of one's time this week and next week fiddling around on your website and you won't find a copyright infringement policy; agree?---There is a page which has copyright breach information and information about iiNet [sic] position on this and the one you referred to earlier on has got an email address, phone number and contact details for the copyright officer.

…

And where is that policy written down?---The policy-well, the right to do it is encompassed in our CRA.

Just pausing there. That is referring then to a contractual obligation?---It's the right to be able to do it where someone is found to have infringed.

You understand a difference between the term of a contract and a policy?---Yes.

Now, that is not the policy, is it?---A term of a contract may be evidence of a policy.

614 In further cross-examination, Mr Malone made clear that the detail of the policy does not exist other than in his mind, though Mr Dalby was aware of it as well. He stated that the termination of subscriber accounts would occur in three circumstances: when the respondent was ordered to do so by a Court; when an iiNet user admitted to infringing copyright; and when an iiNet user was found by a Court or other authority to have infringed. Despite strident assertions to the contrary by the applicants, Mr Malone's cross-examination does establish the third circumstance and it was not proffered only in re-examination as was incorrectly submitted in the applicants' closing submissions in reply:

What is the policy?---If someone is found to infringe on multiple occasions then we may disconnect them.

…

And what constitutes a repeat infringer is not specified?---It's someone who is found to have been – someone is found by a court or other competent authority to have infringed.

…

What does the policy [say] about a customer admitting copyright infringement?---We've already confirmed that we don't have a written policy, so the policy doesn't say anything about it, but my position would be that if someone – they only way someone could be found to have infringed was where they whether were found so by a court or where they admitted to doing so.

…

So the policy you are referring to comes back to some court order, is it?---Yes.

And that is it?---Yes.

You will only – your policy is you won't do anything without a court order?---Sorry, pardon me. The person would be found not by a court order, but by a court saying yes, that person is guilty.

And again, I put it to you, you don't have any repeat infringer policy, do you?---the policy would be, as I said, if someone is found to repeat an infringement – on multiple occasions, then we need to take action.

615 This policy, albeit not wholly written, would satisfy all the requirements outlined in *In re Aimster* 252 FSupp2d 634. The submissions by the applicants that such policy does not exist given that it is not recorded in writing; does not provide for prescriptive steps as stipulated in other ISP's policies (for example Beagle and People Telecom which were exhibited before the Court); and is not communicated to iiNet's users, fails in light of the US authority outlined above, particularly *Corbis*. The policy need not be written, since there is no statutory requirement that a policy be in written form. It need not provide clear steps leading to termination. It need not mention 'repeat infringer'. Parliament, by the absence of any prescription for the policy, saw fit to grant CSPs significant latitude to formulate their own policies.

616 Further, the policy need not be communicated to a CSP's users, given that, as explained, condition 1 of item 1 in s 116AH(1) excluded any requirement for the notification of that policy, unlike 17 USC §512(i)(1)(A) on which condition 1 was clearly modelled. Consequently, the Court rejects the premise of this line of questioning put to Mr Malone:

> Do you understand the purpose of the policy is to inform existing and potential customers as to what iiNet's approach is?---That may be part of the policy' purpose, yes.
>
> And what, you are not going to tell anybody whether they have breached the policy or not, until they have done something which is in breach of a policy they don't know exists. Is that the position?---Sorry, the policy first is don't infringe at all. There is a secondary step which is yes, you have infringed, how do we deal with multiple infringers.

617 As already mentioned, the Court does not draw any inferences from the fact that Mr Dalby did not mention the repeat infringer policy. As already referred to, he was not asked about it in cross-examination. This was, no doubt, a reasonable forensic decision on the part of the applicants, but it does not lead the Court to conclude that he had nothing to say which would have assisted Mr Malone.

618 The applicants' reliance on *Commercial Union Assurance Company of Australia Ltd v Ferrcom Pty Ltd and Another* (1991) 22 NSWLR 389 at 418-419 is misconceived. In that proceeding a *Jones v Dunkel* inference was drawn where there was no direct evidence on a topic *at all* in the hearing and a witness who would have been able to provide evidence in chief about the topic did not do so. This case is different. There is direct evidence of the repeat infringer policy from Mr Malone.

619 The Court finds that the respondent's notification that copyright infringement may lead to termination of subscriber accounts (extracted above at [612]) put the iiNet users on sufficient notice that the respondent had a policy in relation to repeat copyright infringement, and that Mr Malone's understanding of the factors necessary to take action under that policy is sufficient to constitute a repeat infringer policy for the purposes of condition 1 of item 1 of s 116AH(1).

Has the respondent reasonably implemented such a policy?

620 Despite the above, while the Copyright Act gives CSPs significant latitude in the adoption of a repeat infringer policy and therefore its implementation, the text of item 1 condition 1 of s 116AH(1) in the Copyright Act suggests that the requirements of such policy are not entirely at the whim of the CSP:

> The carriage service provider must adopt and **reasonably** implement a policy that provides for termination, in **appropriate circumstances**, of the accounts of repeat infringers. [emphasis added]

The inclusion of the words '*reasonably*' and '*appropriate circumstances*' provide scope for the Court to adjudge a policy and its operation, and that objective element is particularly relevant in an assessment of whether a CSP has implemented a repeat infringer policy that has been adopted by it.

621 The Court finds that the respondent has reasonably implemented a repeat infringer policy. Mr Malone's statement that he has not encountered a circumstance where he has been required to implement the repeat infringer policy was not a '*joke*' (as it was put to him) but is entirely consistent with the policy, given that, as far as the Court is aware, no specific iiNet user has yet been found to have infringed copyright by a Court (before this judgment), and the respondent has not been ordered to terminate a subscriber account by a Court.

622 While the respondent's requirement that an iiNet user be found to have repeatedly infringed copyright by a court sets a high bar before the respondent will effect an iiNet user's termination, the Court believes that, in the circumstances of category A, this is an appropriate policy. In order to understand the Court's approach, reference must first be had to other categories of activity.

623 First, it is to be noted that the Copyright Act and the Regulations create a highly prescriptive regime for dealing with allegedly infringing material in relation to categories B-D. For example, regs 20D-20U provide a regime for dealing with allegations of infringement, notification of those allegations and takedown of infringing materials. In relation to category C activities, reg 20I allows a copyright owner or agent thereof only to provide a notification of claimed infringement in a prescribed form to a CSP. Regulation 20J then provides that the CSP must take down the material and inform the person who uploaded the material. Regulation 20K then allows that person to issue a counter-notice to the CSP stating that the material is not infringing. Following receipt of such notice the CSP must, pursuant to reg 20L, send that notice to the copyright owner, and pursuant to reg 20M, restore the material if the copyright owner does not commence an action within 10 days to have the material restrained or, alternatively, following a suit for copyright infringement which is unsuccessful.

624 Importantly, all notifications pursuant to the regulations are contingent on reg 20X. Such regulation states:

> (1) A person who issues a notification, notice or counter-notice under this Part, for the purpose of satisfying a condition in Subdivision D of Division 2AA of Part V of the Act, must not knowingly make a material misrepresentation in that notification, notice or counter-notice.
>
> (2) For subregulation (1), a person knowingly makes a material misrepresentation in a notification, notice or counter-notice if the person does not take reasonable steps to ensure the accuracy of the information and statements included in the notification, notice or counter-notice.
>
> (3) A person who suffers loss or damage because of a material misrepresentation made knowingly in a notification, notice or counter-notice may bring an action for a civil remedy against the person who issued the notification, notice or counter-notice.

Further, s 137.2 of the *Criminal Code 1995* (Cth) makes it an offence to issue a notification knowing that it is false or misleading in a material particular.

625 The scheme of the Act in respect of other than category A circumstances provides important safeguards in that any copyright owner or agent thereof who makes an allegation of infringement is liable and accountable for that allegation should it be found to knowingly be false, or if reasonable steps are not taken to ensure the accuracy of the allegation. It ensures that CSPs can act upon the assumption that what is presented to them is true, and that they do not need to second guess or speculate upon the validity of the content of the allegation. It

protects those against whom false allegations are made by allowing them to bring suit for that false allegation. It provides certainty for copyright owners by providing a standard which they must meet in order to make the allegation.

626 Second, the nature of categories B-D are such that the allegedly infringing material is stored on the CSP's servers. Therefore, the CSP can usually directly access the material and make an assessment themselves whether the material is infringing. Indeed, regs 20N-20R allow CSPs to take down material they believe to be infringing absent notification by a copyright owner. Category A activities, by their very nature, are transient. Consequently, the CSP cannot independently verify the correctness of the claimed infringement. Of course it was possible to consult the DVD attached to the AFACT Notices, but such evidence was gathered directly by the person making the allegation of infringement and thus would not independently verify the allegations.

627 Arising from this statutory scheme, the Court considers that, at least in relation to category A activities, a repeat infringer policy should necessarily require a high standard of proof before a decision is made by the CSP that one of its users is a repeat infringer with the consequence that their account is terminated. In relation to categories B-D, the notification/counter-notification scheme together with the ability to access the alleged infringing material itself provides the CSPs with a degree of certainty that prescribed conduct is occurring or has occurred absent an independent third party, such as a court, dealing with the matter. In those circumstances a CSP would be able to conclude more readily that a person is repeatedly infringing in relation to those activities and to proceed confidently to terminate their account without the need for any adjudication of a Court.

628 However, a CSP, in relation to category A activities, has a right to be more cautious before accepting the allegations of the copyright owner or an agent thereof. As Lasnik J in *Corbis* found, notices alleging copyright infringement are not the '*sine qua non of copyright liability*' and that '*notices alone do not make the user's activity blatant, or even conclusively determine that the user is an infringer*'. The regulations allow certain assumptions to be made about prescribed notices for categories B-D inclusive, but there is no such scheme for the notices regarding category A activities.

629 The AFACT notifications are not statutory declarations, nor do they have any statutory basis. At no point did Mr Gane swear to the truth of the allegations contained in such Notices. At no point does he state that he personally had taken reasonable steps to ensure that the information and statements in the notice were true and accurate. All these things are required by the prescribed form of notices in the Regulations in categories B-D. The AFACT Notice of 23 July 2008 states:

> AFACT is **associated** with the Motion Picture Association (MPA), whose members include Buena Vista International, Inc, Paramount Pictures Corporation, Sony Pictures Releasing International Corporation, Twentieth Century Fox International Corporation, Universal International Films Inc, and Warner Bros. Pictures International [A Division of Warner Bros. Pictures Inc] and their affiliates. AFACT **represents** Australian producers and/or distributors of cinematographic films and television shows, including affiliates of the member companies of the MPA. AFACT's **members and their affiliates** are either the owners or exclusive licensees of copyright in Australia in the majority of commercially released motion pictures including movies and television shows. AFACT undertakes investigations of infringements of copyright in these movies and television shows. [emphasis added]

As the emphasised sections demonstrate, it is not necessarily clear whether AFACT or Mr Gane is acting as an agent on behalf of the copyright owners or exclusive licensees in making the allegations of infringement (the evidence of Mr Gane and the studio witnesses was that AFACT was not an agent of the applicants). On the face of the letter it is unclear what precise legal relationship AFACT actually has with the copyright owners or exclusive licensees who would necessarily be the ones bringing suit for copyright infringement. Indeed, Roadshow Films and Village Roadshow, the first and twelfth applicants to these proceedings, are not even mentioned in the letter. The letter is concluded with '*[t]his letter is without prejudice to the rights and remedies of the AFACT member companies and their affiliates, which rights are expressly reserved*', further casting doubt in the CSP's mind of the extent to which AFACT can speak for the copyright owners and exclusive licensees. The tone of the letter is not so much that AFACT is an agent of copyright owners, but rather seeks to imply that AFACT is some form of quasi-statutory body whose requests required compliance.

630 It would be perverse for the requirements and obligations imposed upon a copyright owner in making an allegation of copyright infringement to be lower in relation to category A than categories B-D, when, unlike categories B-D, the allegation cannot be independently verified by the CSP. It would not seem to accord with Parliament's intention that safeguards exist, as evidenced by the preceding discussion in regards to the Regulations. The

consequence would be termination of a subscriber account which is a severe consequence. Such considerations must be relevant for an assessment of what are '*appropriate circumstances*' to justify the termination of a subscriber account, and what constitutes implementation of a repeat infringer policy. Consequently, the Court finds that the respondent's repeat infringer policy, at least in relation to category A activities, was reasonably implemented.

631 In summary, the Court finds that it would not be appropriate to construe the safe harbour provisions such that there is an expectation on the CSP to terminate its subscribers at the request of a person who does not swear to the truth of his statement, and is an employee of an organisation whose precise legal status vis-à-vis the relevant copyright owners and exclusive licensees is not at all clear. Allegations of copyright infringement are serious charges which are potentially defamatory. Further, AFACT enjoys no status as an authority invested with power to issue legally enforceable directions. Merely because there is no statutory scheme regarding category A does not lead to the consequence that the considerations underlying the notification/counter-notification scheme in categories B-D are not relevant to the Court's determination of what is a reasonable implementation of a repeat infringer policy.

632 Finally on this issue, the Court rejects the submissions of the applicants that *Ellison* 357 F3d 1072 and *Aimster* 252 FSupp2d 634 require the Court to find that the respondent did not reasonably implement a repeat infringer policy. Those authorities concerned service providers taking *positive* steps to prevent any repeat infringer policy being implemented. In the first case it was a decision to change an email address without suitable notification or a mechanism to have the emails on-forwarded; in the second it was encryption of the system such that it was impossible to connect user and transmission. In these proceedings, it is not the respondent's positive steps that the applicants complain of, but a lack of positive steps. The Court finds that the cases referred to are inapposite.

Other issues

633 The respondent has submitted that as condition 1 of item 1 is phrased as '*…accounts of repeat infringers*' the only appropriate circumstance to terminate an account would be where the repeat infringer was the account holder himself or herself. As has been explained in

this judgment, this may not be the case. However, the Court rejects the respondent's submission. The wording in the safe harbour EM at 161 is broader, stating '*the accounts of users who are repeat copyright infringers*'. Further, there is no suggestion in the US authorities that the infringer has to be the account holder themselves. Such a construction would make it difficult for a CSP to take advantage of the safe harbour, because in order to terminate only account holders who infringe, following an allegation of infringement the CSP would have to establish the identity of the actual infringer.

Conclusion

634 For all the reasons outlined above, should the Court be found to have erred in its finding regarding authorisation, the Court would find that the respondent has adopted and reasonably implemented a repeat infringer policy, and has consequently satisfied the requirements of the Division 2AA of Part V of the Copyright Act. Therefore, the orders the Court could make would be limited to those found in s 116AG(3) of the Copyright Act. However, as the Court has found that the respondent has not authorised infringement, and liability does not arise, there is no occasion to consider any appropriate remedies.

PART G: CONCLUSION

635 The Court makes the following findings:

(1) The Court finds that primary infringement has been made out. The applicants have proven that the iiNet users 'made available online', 'electronically transmitted' and made copies of the identified films.

(2) The Court finds that the applicants have not proven that the respondent authorised the infringement of the iiNet users. In making such finding the Court finds that Telco Act defence does not arise, and the Court finds that s 112E is not applicable in the present circumstances. Consequently, the Amended Application fails.

(3) The Court finds that the respondent satisfied the requirements of the safe harbour provisions, though, because of the finding in (2), it does not need their protection.

636 Therefore the Amended Application of the applicants fails. The Court will make an order that the applicants pay the respondent's costs in the matter, as well as the costs thrown away by the respondent due to the applicants abandoning of the primary infringement claim against the respondent. Should any party wish to make further submissions on the issue of costs they have leave to notify the Court within 14 days.

I certify that the preceding six hundred and thirty-six (636) numbered paragraphs are a true copy of the Reasons for Judgment herein of the Honourable Justice Cowdroy.

Associate:

Dated: 4 February 2010

SCHEDULE I – THE APPLICANTS

UNIVERSAL CITY STUDIOS LLLP
Second Applicant

PARAMOUNT PICTURES CORPORATION
Third Applicant

WARNER BROS. ENTERTAINMENT INC.
Fourth Applicant

DISNEY ENTERPRISES, INC.
Fifth Applicant

COLUMBIA PICTURES INDUSTRIES, INC
Sixth Applicant

TWENTIETH CENTURY FOX FILM CORPORATION
Seventh Applicant

PARAMOUNT HOME ENTERTAINMENT (AUSTRALASIA) PTY LTD
Eighth Applicant

BUENA VISTA HOME ENTERTAINMENT, INC.
Ninth Applicant

TWENTIETH CENTURY FOX FILM CORPORATION (AUSTRALIA) PTY LIMITED
Tenth Applicant

UNIVERSAL PICTURES (AUSTRALIA) PTY LTD
Eleventh Applicant

VILLAGE ROADSHOW FILMS (BVI) LTD
Twelfth Applicant

UNIVERSAL PICTURES INTERNATIONAL B.V
Thirteenth Applicant

UNIVERSAL CITY STUDIOS PRODUCTIONS LLLP
Fourteenth Applicant

RINGERIKE GMBH & CO KG
Fifteenth Applicant

INTERNATIONALE FILMPRODUKTION BLACKBIRD VIERTE GMBH & CO KG
Sixteenth Applicant

MDBF ZWEITE FILMGESELLSCHAFT MBH & CO KG
Seventeenth Applicant

INTERNATIONALE FILMPRODUCKTION RICHTER GMBH & CO KG
Eighteenth Applicant

NBC STUDIOS, INC
Nineteenth Applicant

DREAMWORKS FILMS L.L.C
Twentieth Applicant

WARNER BROS INTERNATIONAL TELEVISION DISTRIBUTION INC
Twenty-First Applicant

TWENTIETH CENTURY FOX HOME ENTERTAINMENT INTERNATIONAL CORPORATION
Twenty-Second Applicant

WARNER HOME VIDEO PTY LTD
Twenty-Third Applicant

PATALEX III PRODUCTIONS LIMITED
Twenty-Fourth Applicant

LONELY FILM PRODUCTIONS GMBH & CO KG
Twenty-Fifth Applicant

SONY PICTURES ANIMATION INC
Twenty-Sixth Applicant

UNIVERSAL STUDIOS INTERNATIONAL B.V.
Twenty-Seventh Applicant

SONY PICTURES HOME ENTERTAINMENT PTY LTD
Twenty-Eighth Applicant

GH ONE LLC
Twenty-Ninth Applicant

GH THREE LLC
Thirtieth Applicant

BEVERLY BLVD LLC
Thirty-First Applicant

WARNER BROS ENTERTAINMENT AUSTRALIA PTY LTD
Thirty-Second Applicant

TWENTIETH CENTURY FOX HOME ENTERTAINMENT LLC
Thirty-Third Applicant

SEVEN NETWORK (OPERATIONS) LTD
Thirty-Fourth Applicant

SCHEDULE II – THE IDENTIFIED FILMS

No.	Title	Owner(s)	Exclusive licensee(s)
Roadshow Films			
R1	*I Am Legend*	Village Roadshow Films (BVI) Limited	Roadshow Films Pty Ltd
R2	*Speed Racer*	Village Roadshow Films (BVI) Limited	Roadshow Films Pty Ltd
R3	*Happy Feet*	Village Roadshow Films (BVI) Limited	Roadshow Films Pty Ltd
R4	*The Invasion*	Village Roadshow Films (BVI) Limited	Roadshow Films Pty Ltd
R5	*Ocean's 13*	Village Roadshow Films (BVI) Limited	Roadshow Films Pty Ltd
R6	*The Reaping*	Village Roadshow Films (BVI) Limited	Roadshow Films Pty Ltd
R7	*No Reservations*	Village Roadshow Films (BVI) Limited	Roadshow Films Pty Ltd
R8	*The Brave One*	Village Roadshow Films (BVI) Limited	Roadshow Films Pty Ltd
Universal Films			
U1	*Forgetting Sarah Marshall*	Universal City Studios Productions LLLP	Universal Studios International BV Universal Pictures (Australasia) Pty Ltd
U2	*American Gangster*	Universal City Studios Productions LLLP	Universal Studios International BV Universal Pictures (Australasia) Pty Ltd
U3	*The Mummy: Tomb of the Dragon Emperor*	Universal City Studios Productions LLLP	Universal Studios International BV

No.	Title	Owner(s)	Exclusive licensee(s)
		Ringerike GmbH & Co KG	Universal Pictures (Australasia) Pty Ltd
U4	*Wanted*	Universal City Studios Productions LLLP Internationale Filmproduktion Blackbird Vierte GmbH & Co KG	Universal Studios International BV Universal Pictures (Australasia) Pty Ltd
U5	*Atonement*	Universal City Studios Productions LLLP	Universal Studios International BV Universal Pictures (Australasia) Pty Ltd
U6	*The Kingdom*	Universal City Studios Productions LLLP MDBF Zweite Filmgesellschaft mbH & Co KG	Universal Studios International BV Universal Pictures (Australasia) Pty Ltd
U7	*Baby Mama*	Universal City Studios Productions LLLP	Universal Studios International BV Universal Pictures (Australasia) Pty Ltd
U8	*Mamma Mia!*	Universal City Studios Productions LLLP Internationale Filmproduktion Richter GmbH & Co KG	Universal Studios International BV Universal Pictures (Australasia) Pty Ltd
U9	*Heroes*, Season 3, Episode 3, "One of Us, One of Them"	NBC Studios Inc	Universal Studios International BV Universal Pictures (Australasia) Pty Ltd Seven Network (Operations) Limited
U10	*Heroes*, Season 3, Episode 4, "I	NBC Studios Inc	Universal Studios International

No.	Title	Owner(s)	Exclusive licensee(s)
	Am Become Death”		BV Universal Pictures (Australasia) Pty Ltd Seven Network (Operations) Limited
U11	*Heroes*, Season 3, Episode 5, “Angels and Monsters”	NBC Studios Inc	Universal Studios International BV Universal Pictures (Australasia) Pty Ltd Seven Network (Operations) Limited
U12	*Life*, Season 2, Episode 3, “The Business of Miracles”	NBC Studios Inc	Universal Studios International BV Universal Pictures (Australasia) Pty Ltd
Paramount Films			
P1	*The Spiderwick Chronicles*	Paramount Pictures Corporation	Paramount Home Entertainment (Australasia) Pty Ltd
P2	*Cloverfield*	Paramount Pictures Corporation	Paramount Home Entertainment (Australasia) Pty Ltd
P3	*Stop-Loss*	Paramount Pictures Corporation	Paramount Home Entertainment (Australasia) Pty Ltd
P4	*Shooter*	Paramount Pictures Corporation	Paramount Home Entertainment (Australasia) Pty Ltd
P5	*Transformers*	Paramount Pictures Corporation DreamWorks Films L.L.C.	Paramount Home Entertainment (Australasia) Pty Ltd
P6	*Hot Rod*	Paramount Pictures Corporation	Paramount Home Entertainment (Australasia) Pty Ltd
P7	*Stardust*	Paramount Pictures Corporation	Paramount Home Entertainment

No.	Title	Owner(s)	Exclusive licensee(s)
			(Australasia) Pty Ltd
P8	*The Heartbreak Kid*	DreamWorks Films L.L.C.	Paramount Home Entertainment (Australasia) Pty Ltd
P9	*Things We Lost in the Fire*	DreamWorks Films L.L.C.	Paramount Home Entertainment (Australasia) Pty Ltd
Warner Bros Films			
WB1	*Batman Begins*	Warner Bros Entertainment Australia Pty Ltd	
WB2	*Gossip Girl*, Season 2, Episode 2, "Never Been Marcused"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
WB3	*Supernatural*, Season 3, Episode 15, "Time Is On My Side"	Warner Bros Home Entertainment Inc Warner Bros Entertainment Australia Pty Ltd	
WB4	*300*	Warner Bros Entertainment Australia Pty Ltd Warner Bros International Television Distribution Inc	
WB5	*Blood Diamond*	Warner Bros Entertainment Australia Pty Ltd Warner Bros International Television Distribution Inc	
WB6	*One Tree Hill*, Season 6, Episode 2, "One Million Billionth of a Millisecond on a Sunday Morning"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
WB7	*Harry Potter and the Order of the Phoenix*	Warner Bros Entertainment Australia Pty Ltd	

No.	Title	Owner(s)	Exclusive licensee(s)
		Warner Bros International Television Distribution Inc	
WB8	*The Closer*, Season 4, Episode 6, "Problem Child"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
WB9	*Smallville*, Season 7, Episode 17, "Sleeper"	Warner Bros Home Entertainment Inc Warner Bros Entertainment Australia Pty Ltd	
WB10	*Two and a Half Men*, Season 5, Episode 19, "Waiting for the Right Snapper"	Warner Bros Home Entertainment Inc Warner Bros Entertainment Australia Pty Ltd	
WB11	*Gossip Girl*, Season 2, Episode 1, "Summer, Kind of Wonderful"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
WB12	*Supernatural*, Season 4, Episode 1, "Lazarus Rising"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
WB13	*Supernatural*, Season 4, Episode 2, "Are you There God? It's Me, Dean Winchester"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
WB14	*Supernatural*, Season 4, Episode 3, "In the Beginning"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	

No.	Title	Owner(s)	Exclusive licensee(s)
WB15	*One Tree Hill*, Season 6, Episode 1, "Touch Me, I'm Going to Scream"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
WB16	*One Tree Hill*, Season 6, Episode 3, "Get Cape. Wear Cape. Fly"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
WB17	*Smallville*, Season 8, Episode 1, "Odyssey"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
WB18	*Smallville*, Season 8, Episode 2, "Plastique"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
WB19	*Smallville*, Season 8, Episode 3, "Toxic"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
WB20	*Smallville*, Season 8, Episode 4, "Instinct"	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
WB21	*Two and a Half Men*, Season 5, Episode 16, "Look At Me, Mommy, I'm Pretty"	Warner Bros Home Entertainment Inc Warner Bros Entertainment Australia Pty Ltd	
WB22	*Two and a Half Men*, Season 5, Episode 17, "Fish in a Drawer"	Warner Bros Home Entertainment Inc	

No.	Title	Owner(s)	Exclusive licensee(s)
		Warner Bros Entertainment Australia Pty Ltd	
WB23	*The Dark Knight*	Warner Bros Home Entertainment Inc Warner Bros International Television Distribution Inc	
Disney Films			
D1	*Enchanted*	Disney Enterprises, Inc	Buena Vista Home Entertainment, Inc
D2	*Pirates of The Caribbean: At World's End*	Disney Enterprises, Inc	Buena Vista Home Entertainment, Inc
D3	*College Road Trip*	Disney Enterprises, Inc	Buena Vista Home Entertainment, Inc
Columbia Films			
C1	*Hancock*	Columbia Pictures Industries, Inc GH Three LLC	Sony Pictures Home Entertainment Pty Ltd
C2	*21*	Columbia Pictures Industries, Inc GH Three LLC	Sony Pictures Home Entertainment Pty Ltd
C3	*Spider-Man 3*	Columbia Pictures Industries, Inc	Sony Pictures Home Entertainment Pty Ltd
C4	*Made of Honor* (also known as *Made of Honour*)	Columbia Pictures Industries, Inc Beverly Blvd LLC	Sony Pictures Home Entertainment Pty Ltd
C5	*Talladega Nights: The Ballad of Ricky Bobby*	Columbia Pictures Industries, Inc GH One LLC	Sony Pictures Home Entertainment Pty Ltd

No.	Title	Owner(s)	Exclusive licensee(s)
C6	*Vantage Point*	Columbia Pictures Industries, Inc GH Three LLC	Sony Pictures Home Entertainment Pty Ltd
C7	*Surf's Up*	Sony Animation Inc	Sony Pictures Home Entertainment Pty Ltd
C8	*Superbad*	Columbia Pictures Industries, Inc	Sony Pictures Home Entertainment Pty Ltd
C9	*The Pursuit of Happyness*	Columbia Pictures Industries, Inc GH One LLC	Sony Pictures Home Entertainment Pty Ltd
C10	*Pineapple Express*	Columbia Pictures Industries, Inc Beverly Blvd LLC	Sony Pictures Home Entertainment Pty Ltd
Fox Films			
F1	*Dr Seuss' Horton Hears A Who!*	Twentieth Century Fox Home Entertainment LLC	Twentieth Century Fox Home Entertainment International Corporation
F2	*Night At The Museum*	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation
F3	*The Simpsons*, Season 19, Episode 17, "Apocalypse Cow"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation
F4	*The Simpsons*, Season 19, Episode 18, "Any Given Sundance"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation

No.	Title	Owner(s)	Exclusive licensee(s)
F5	*The Simpsons*, Season 19, Episode 19, "Mona Leaves-A"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation
F6	*The Simpsons*, Season 19, Episode 20, "All About Lisa"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation
F7	*Family Guy*, Season 7, Episode 1, "Love Blactually"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited
F8	*Family Guy*, Season 7, Episode 2, "I Dream of Jesus"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited
F9	*Family Guy*, Season 7, Episode 3, "Road to Germany"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited
F10	*Prison Break*, Season 4, Episode 1, "Scylla"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited

No.	Title	Owner(s)	Exclusive licensee(s)
F11	*Prison Break*, Season 4, Episode 3, "Shut Down"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited
F12	*Prison Break*, Season 4, Episode 4, "Eagles and Angels"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corp Seven Network (Operations) Limited
F13	*Bones*, Season 4, Episodes 1-2, "Yanks in the UK Part 1" and "Yanks in the UK Part 2"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited
F14	*Bones*, Season 4, Episode 3, "The Man in the Outhouse"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited
F15	*Bones*, Season 4, Episode 4, "The Finger in the Nest"	Twentieth Century Fox Film Corporation Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited
F16	*Bones*, Season 4, Episode 6, "The Crank in the Shaft"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited

No.	Title	Owner(s)	Exclusive licensee(s)
F17	*Bones*, Season 4, Episode 7, "The He in the She"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited
F18	*Family Guy*, Season 6, Episode 11, "The Former Life of Brian"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited
F19	*How I Met Your Mother*, Season 4, Episode 3, "I Heart NJ"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited
F20	*American Dad*, Season 4, Episode 2, "The One That Got Away"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited
F21	*American Dad*, Season 4, Episode 3, "One Little Word"	Twentieth Century Fox Home Entertainment LLC Twentieth Century Fox Film Corporation (Australia) Pty Ltd	Twentieth Century Fox Home Entertainment International Corporation Seven Network (Operations) Limited