FEDERAL COURT OF AUSTRALIA

Roadshow Films Pty Limited v iiNet Limited [2011] FCAFC 23

Citation:	Roadshow Films Pty Limited v iiNet Limited [2011] FCAFC 23
Appeal from:	Roadshow Films Pty Ltd v iiNet Limited (No. 3) [2010] FCA 24
Parties:	**ROADSHOW FILMS PTY LIMITED (ACN 100 746 870) and PARTIES IN ATTACHED SCHEDULE 1 v IINET LIMITED (ACN 068 628 937)**
File number:	NSD 179 of 2010
Judges:	**EMMETT, JAGOT AND NICHOLAS JJ**
Date of judgment:	24 February 2011
Catchwords:	**INTELLECTUAL PROPERTY** – authorisation of copyright infringement – copyright infringement notices served on internet service provider (ISP) alleging that users of ISP's network were infringing copyright in cinematographic films by making them available online and electronically transmitting them to the public– whether ISP authorised copyright infringement – whether ISP had power to prevent infringement – whether ISP took reasonable steps to prevent or avoid infringement – consideration of other factors relevant to authorisation – knowledge of infringement – encouragement of infringement – inactivity and indifference to infringement – whether ISP sanctioned, approved or countenanced infringement – whether s 112E of the Copyright Act 1968 (Cth) prevented ISP from being found to have authorised infringement **INTELLECTUAL PROPERTY** – acts of primary infringement – whether users of ISP's network infringed copyright in cinematographic films by making them available online or electronically transmitting them to the public – whether the whole or a substantial part of any such cinematographic film was electronically transmitted – whether individual users committed multiple acts of infringement in relation to any such cinematographic film by making it available online and electronically transmitting it.

INTELLECTUAL PROPERTY – whether Telecommunications Act 1997 (Cth) compelled a finding that ISP could not reasonably be expected to issue warning notices to customers or suspend or terminate their accounts on the basis of the copyright infringement notices because the disclosure or use of information contained in them or business records of the ISP to which it would need to have regard for that purpose was prohibited by law.

INTELLECTUAL PROPERTY – 'safe harbour' provisions – whether ISP complied with relevant provisions of Division 2AA of Part V of the Copyright Act 1968 (Cth)

Legislation:

Copyright Act 1968 (Cth) ss 10, 13, 14(1), 22(6), 22(6A), 31, 39A, 39B, 86, 101, 101(1A), 112E, 115, 116AA, 116AB, 116AC, 116AG and 116AH
Copyright Amendment (Digital Agenda) Act 2000 (Cth) s 3
Copyright Regulations 1969 reg 20B, Schedule 10
Criminal Code Act 1995 (Cth) s 137.2
Federal Court Rules O 13 r 3A and O 52 r 14AA
Telecommunications Act 1997 (Cth) ss 276, 279, 280, 289 and 290

Cases cited:

Adelaide Corporation v Australasian Performing Right Association Ltd (1928) 40 CLR 481
ASIC v Citigroup Global Markets Australia Pty Limited (No.3) [2007] FCA 393
Australasian Performing Right Association Limited v Jain (1990) 26 FCR 53
Australasian Performing Right Association Ltd v Metro on George Pty Ltd (2004) 210 ALR 244
Australian Tape Manufacturers Association Ltd v Commonwealth (1993) 176 CLR 480
Canadian Pacific Tobacco Company Limited v Stapleton (1952) 86 CLR 1
CBS Incorporation v Ames Records and Tapes Ltd [1982] Ch 91
CBS Songs Ltd v Amstrad Consumer Electronics Plc [1988] AC 1013
Colbeam Palmer Ltd v Stock Affiliates Pty Ltd (1968) 122 CLR 25
Cooper v Universal Music Australia Pty Ltd (2006) 156 FCR 380
Falcon v Famous Players Film Co [1926] 2 KB 474
Fox v Percy (2003) 214 CLR 118
IceTV Pty Limited v Nine Network Australia Pty Limited (2009) 239 CLR 458
Levy v State of Victoria (1997) 189 CLR 579
Morton-Norwich Products Inc v Intercen Ltd [1978] RPC

501
Nationwide News Pty Ltd v Copyright Agency Limited (1996) 65 FCR 399
Network Ten Pty Limited v TCN Channel Nine Pty Limited (2004) 218 CLR 273
Performing Right Society Ltd v Cyril Theatrical Syndicate Ltd [1924] 1 KB 1
Project Blue Sky Inc v Australian Broadcasting Authority (1998) 194 CLR 355
Roadshow Films Pty Ltd v iiNet Pty Ltd (No 3) (2010) 263 ALR 215
Sharman Networks Ltd v Universal Music Australia Pty Ltd (2006) 155 FCR 291
Sony Corporation of America v Universal City Studios Inc (1984) 464 US 417
Telstra Corporation Ltd v Australasian Performing Right Association Ltd (1997) 191 CLR 140
The Queen v Crabbe (1985) 156 CLR 464
Universal Music Australia Pty Ltd & Ors v Sharman License Holdings Ltd (2005) 220 ALR 1
Universal Music Australia Pty Ltd v Cooper (2005) 150 FCR 1
University of New South Wales v Moorhouse (1975) 133 CLR 1
WEA International Inc v Hanimex Corporation Ltd (1987) 17 FCR 274

Date of hearing:	2, 3, 4 and 5 August 2010
Date of last submissions:	8 September 2010
Place:	Sydney
Division:	GENERAL DIVISION
Category:	Catchwords
Number of paragraphs:	807
Counsel for the Appellant:	D.K. Catterns QC, J.M. Hennessy and C. Dimitriadis
Solicitor for the Appellant:	Gilbert + Tobin
Counsel for the Respondent:	R. Cobden SC, R.P.L. Lancaster SC and N.R. Murray
Solicitor for the Respondent:	Herbert Geer Lawyers
Counsel for the Media, Entertainment and Arts	M. Hall

Alliance & the Screen Actors Guild:	
Solicitor for the Media, Entertainment and Arts Alliance & the Screen Actors Guild:	Banki Haddock Fiora
Counsel for APRA:	M. Leeming SC
Solicitor for APRA:	Banki Haddock Fiora

IN THE FEDERAL COURT OF AUSTRALIA
NEW SOUTH WALES DISTRICT REGISTRY
GENERAL DIVISION **NSD179 of 2010**

ON APPEAL FROM THE FEDERAL COURT OF AUSTRALIA

BETWEEN:	**ROADSHOW FILMS PTY LIMITED (ACN 100 746 870)** **First Appellant**
	THE PARTIES IN THE ATTACHED SCHEDULE 1 **Second Appellant to Thirty-Fourth Appellant**
AND:	**IINET LIMITED (ACN 068 628 937)** **Respondent**
JUDGES:	**EMMETT, JAGOT AND NICHOLAS JJ**
DATE OF ORDER:	**24 FEBRUARY 2011**
WHERE MADE:	**SYDNEY**

THE COURT ORDERS THAT:

1. The appeal be dismissed.

2. The parties bring in short minutes of proposed directions concerning any argument as to 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 Federal Law Search on the Court's website.

IN THE FEDERAL COURT OF AUSTRALIA
NEW SOUTH WALES DISTRICT REGISTRY
GENERAL DIVISION **NSD179 of 2010**

ON APPEAL FROM THE FEDERAL COURT OF AUSTRALIA

BETWEEN:	**ROADSHOW FILMS PTY LIMITED (ACN 100 746 870)** **First Appellant**
	THE PARTIES IN THE ATTACHED SCHEDULE 1 **Second Appellant to Thirty-Fourth Appellant**
AND:	**IINET LIMITED (ACN 068 628 937)** **RESPONDENT**
JUDGES:	**EMMETT, JAGOT AND NICHOLAS JJ**
DATE:	**24 FEBRUARY 2011**
PLACE:	**SYDNEY**

EMMETT J

REASONS FOR JUDGMENT

INTRODUCTION

1 One or other of the appellants (together **the Copyright Owners**) is the owner of copyright in one or more of a number of cinematograph films (**the Films**). The respondent, iiNet Limited (**iiNet**), is a carriage service provider. That is to say, iiNet provides its customers with access to the internet. It is common ground that, by use of the internet access

services provided to its customers by iiNet, the Copyright Owners' copyright in the Films has been infringed, although there is a dispute as to the precise characterisation of the infringements. The Copyright Owners claim that iiNet has authorised the acts of infringement done by the use of its services. Accordingly, they claim, iiNet itself has infringed their copyrights.

2 The Copyright Owners commenced a proceeding in the Court seeking relief against iiNet in respect of the alleged infringement by iiNet. A judge of the Court concluded that there was no infringement by iiNet and dismissed the proceeding with costs. The Copyright Owners have now appealed from those orders, saying that the primary judge erred in a number of respects. iiNet has filed notice of contention seeking to support the orders made by the primary judge on other grounds.

3 The appeal raises issues under the *Copyright Act 1968* (Cth) (**the Copyright Act**) and the *Telecommunications Act 1997* (Cth) (**the Telco Act**) that are of some significance and complexity. It is common ground that iiNet is a **carriage service provider** within the meaning of the Copyright Act and the Telco Act. Before stating the issues and explaining the somewhat complex technical and factual background against which the issues must be considered, it is desirable to say something about the relevant provisions of the Copyright Act and the Telco Act.

THE RELEVANT STATUTORY PROVISIONS

4 Under s 86 of the Copyright Act, copyright, in relation to a cinematograph film, is the exclusive right to do all or any of the following acts:

- to make a copy of the film;
- to cause the film, in so far as it consists of visual images, to be seen in public, or, in so far as it consists of sounds, to be heard in public; and
- to communicate the film to the public.

Under s 10, **communicate** means, relevantly in relation to a cinematograph film:

- make the film available online, or
- electronically transmit the film.

5 Under s 22(6) and s 22(6A), a communication is taken to have been made by the person responsible for determining the content of the communication. However, 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 gaining access to what is made available online by someone else or receiving the electronic transmission of which the communication consists. For example, a person is not responsible for determining the content of the communication to that person of a web page merely because the person clicks on a link to gain access to the page.

6 Under s 101(1) of the Copyright Act, a person infringes the copyright subsisting in a cinematograph film if the person does an act comprised in the copyright without the consent of the owner of the copyright. Further, copyright subsisting in relation to a cinematograph film is infringed by a person who **authorises** the doing in Australia of any act comprised in the copyright. Section 101(1A) relevantly provides that, in determining, for the purpose of s 101(1), whether or not a person has authorised the doing in Australia of any act comprised in a copyright in relation to a cinematograph film, the following matters **must** be taken into account:

(a) the extent (if any) of the person's power to prevent the doing of the act concerned;

(b) the nature of any relationship existing between the person and the person who did the act concerned; and

(c) whether the person 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.

Those three matters are not the only matters that may be taken into account.

7 Under s 112E of the Copyright Act, a 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, relevantly, a cinematograph film **merely because** another person uses the facilities so provided to do something the right to do which is included in the copyright. The word **communication** in s 112E has a meaning that corresponds with the definition of communicate in s 10. Thus, s 112E qualifies the operation of s 101(1A) when it

is necessary to determine whether a person has authorised the copying in Australia of a film, in circumstances where the relevant copying involves the making available online, or the electronic transmission of, the film by way of facilities provided by that person. Such a person is not taken to have authorised the infringement **merely because** another person uses the facilities provided by the first person to achieve the making of a copy.

8 Division 2AA of Part V of the Copyright Act, which consists of ss 116AA to 116AJ (**the Safe Harbour Provisions**), imposes limitations on the remedies available against carriage service providers for infringement of copyright. The Safe Harbour Provisions were inserted into the Copyright Act by the *US Free Trade Agreement Implementation Act 2004* (Cth) (**the US Free Trade Act**). The purpose of the Safe Harbour Provisions is to limit the remedies that are available against a carriage service provider for infringements of copyright that relate to the carrying out of certain online activities by the carriage service provider.

9 Under s 116AC, a carriage service provider carries out **a Category A activity** by, relevantly, providing facilities or services for transmitting, routing or providing connections for a cinematograph film, or the intermediate and transient storage of a cinematograph film in the course of transmission, routing or provision of connections. Section 116AG(3) relevantly provides that, for an infringement of copyright that occurs in the course of the carrying out of a Category A activity, the relief that the Court may grant against a carriage service provider is limited to one or more of the following:

- an order requiring the carriage service provider to take reasonable steps to disable access to an online location outside Australia; and
- an order requiring the carriage service provider to terminate a specified account.

10 In deciding whether to make an order of the kind referred to in s 116AG(3), the Court must have regard to:

- the harm that has been caused to the owner of the copyright,
- the burden that the making of the order will place on the carriage service provider,

- the technical feasibility of complying with the order,
- the effectiveness of the order, and
- whether some other comparably effective order would be less burdensome.

The Court may also have regard to other matters that the Court considers relevant.

11 However, under s 116AG(1), before the limitations in s 116AG(3) apply, a carriage service provider must satisfy certain conditions. Relevantly, the conditions for category A activities of carriage service providers are set out in the table in s 116AH(1). The first condition in the table in s 116AH(1) is that the carriage service provider must adopt and reasonably implement a policy (**Termination Policy**) that provides for termination, in appropriate circumstances, of the accounts of **repeat infringers**.

12 Another condition is that, 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. Under s 116AB, an **industry code** is one that meets any prescribed requirements and is registered under the Telco Act or one developed in accordance with the *Copyright Regulations 1969* (Cth) (**the Regulations**). Section 116AH(2) provides that nothing in those 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 that is the subject of an industry code. It is common ground that, at relevant times, there was no relevant industry code in force.

13 iiNet also relies, if necessary, on the provisions of Part 13 of the Telco Act as constituting an answer to any obligation to take steps to prevent an alleged infringement of copyright by its customers. Part 13, which includes ss 270 to 310 inclusive, deals with the protection of communications. Under Part 13, a carriage service provider must protect the confidentiality of information that relates to:

- the contents of communications that have been, or are being, carried by the carriage service provider,
- carriage services supplied by the carriage service provider, and
- the affairs or personal particulars of other persons.

14 To that end, s 276(1) relevantly provides that a service carriage provider must not disclose or use any information or document that:

(a) relates to:

- the contents or substance of a communication that has been carried by the carriage service provider,
- carriage services provided, or intended to be supplied, to another person by the carriage service provider, or
- the affairs or personal particulars of another person, **and**

(b) comes to the knowledge or into the possession of the carriage service provider in connection with the carriage service provider's business as a carriage service provider.

15 Section 276(3) provides that a person who contravenes s 276(1) is guilty of an offence. However, Division 3 of Part 13, which consists of ss 279 to 294 inclusive, provides for exceptions to the prohibition in s 276. Four provisions are relied on by the Copyright Owners.

16 The first is s 279(1), which provides that s 276 does not prohibit a disclosure or use by a person of information or a document if:

- the person is an employee of a carriage service provider, and
- the disclosure or use is made in the performance of the person's duties as such an employee.

17 Second, under s 280(1), s 276 does not prohibit a disclosure or use of information or a document if, relevantly, the disclosure or use is required or authorised by or under law. Third, under s 289, s 276 does not prohibit a disclosure or use by a person of information or a document if:

- the information or document relates to the affairs or personal particulars of another person, and

- the other person, relevantly, has consented to the disclosure or use, as the case requires, in the circumstances concerned.

Finally, under s 290, s 276 does not prohibit a disclosure or use by a person if:

- the information or document relates to the context or substance of a communication made by another person, and
- having regard to all the relevant circumstances, it might reasonably be expected that the sender and recipient of the communication would have consented to the disclosure or use, if they had been aware of the disclosure or use.

RELEVANT LEGAL PRINCIPLES

18 Section 101(1A) was inserted into the Copyright Act by the *Copyright Amendment (Digital Agenda) Act 2000* (Cth) (**the Digital Agenda Act**). Section 112E was also inserted into the Copyright Act by the Digital Agenda Act. The Digital Agenda Act also inserted into s 10 of the Copyright Act the definition of **communicate**.

19 The objects of the Digital Agenda Act, as stated in s 3, included the following:

- to ensure the efficient operation of relevant industries in the online environment;
- to promote certainty for information technology industries that are investing in and providing online access to copyright material;
- to provide reasonable access and certainty for internet users of copyright material online; and
- to ensure the promotion of new technologies.

However, the Digital Agenda Act did not disclose a legislative intention to alter the meaning of the word authorises in the context of the Copyright Act.

20 Section 101(1A) recognises that an element of judgment is involved in determining whether one person has, for the purposes of s 101(1), authorised another to do a particular act. Section 101(1A) discloses an intention to guard the process by which the judgment is reached as to whether a person authorises the doing in Australia of an act comprised in the

copyright. The decision maker must have regard to the matters identified in s 101(1A), which have particular relevance where the alleged act of infringement has occurred online (see *Cooper v Universal Music Pty Ltd* (2006) 156 FCR 380 (***Cooper's Case***) at [19] and [20]).

21 Section 101(1A) was introduced with an object of providing a practical enforcement regime for copyright owners in the online environment (see *Cooper's Case* at [135]). Accordingly, the question of authorisation must be determined primarily by reference to s 101(1A). The appropriate starting point, therefore, is to have regard to the matters referred to in that provision (see *Cooper's Case* at [28]).

22 The inclusion of the three matters referred to in s 101(1A) was intended to codify certain principles in relation to authorisation that then existed at common law. That inclusion was intended to provide a degree of certainty about the steps that should be taken in order to avoid liability for authorising infringements.

23 The language of s 101(1A) is reminiscent of language to be found in the reasons of the High Court in *University of New South Wales v Moorhouse* (1975) 133 CLR 1 (***Moorhouse***). Accordingly, the principles propounded in *Moorhouse* must be taken to have been given attention by the Parliament when enacting s 101(1A). It is therefore important to have regard to those principles.

24 The word **authorise**, when used in s 101, has its dictionary meaning of **sanction**, **approve** or **countenance**. There is no reason to understand the phrase **sanction, approve or countenance** as importing an element of official approval. Express or formal permission or active conduct indicating approval is not essential to constitute authorisation with s 101(1) (see *WEA International Inc v Hanimex Corporation Ltd* (1987) 17 FCR 274 (***Hanimex***) at 286). Official approval is fundamentally different from the concept of countenancing.

25 Authorise can also mean **permit,** since the words **authorise** and **permit** are often treated as synonymous. However, a person cannot be said to authorise an infringement of copyright unless that person has some power to prevent it. Nevertheless, express or formal permission or sanction or active conduct indicating approval is not essential to constitute an authorisation. Inactivity or indifference, exhibited by acts of commission or omission, may

reach a degree from which an authorisation or permission may be inferred, although the word **authorise** connotes a mental element. It cannot be inferred, from mere inactivity by a person, that the person had authorised something to be done, if the person neither knew, nor had reason to suspect, that the act might be done. Indifference or omission will not be permission unless the party sought to be made liable, amongst other things, knows, or has reason to know or believe, that the particular act in the copyright will or may be done (see *Moorhouse* at 12-13).

26 A person who has under that person's control the means by which an infringement of copyright may be committed and who makes that means available to another person, knowing, or having reason to suspect, that the means is likely to be used for the purpose of committing an infringement and who omits to take reasonable steps to limit use of the means to legitimate purposes, authorises any infringement that results from the use of that means. There will be authorisation where the person sought to be made liable knows or has reason to suspect that a class or category of acts in the copyright might be done (see *Moorhouse* at 13).

27 The word **authorise** in s 101 is not limited to the authorising of an agent by a principal to do an act in the copyright of material. Where there is such an authority, the act of the agent is the act of the principal and thus the principal may be said to do the act comprised in the copyright. However, authorisation is wider than authority. It has a wide meaning that, in cases of permission or invitation, is apt to apply both where an express permission or invitation is extended to do an act comprised in copyright and where such a permission or invitation may be implied. Where a general permission or invitation may be implied, it is unnecessary that the authorising party have knowledge that a particular act comprised in the copyright will be done (see *Moorhouse* at 21).

28 The manufacture and sale of a device that has lawful uses will not constitute authorisation of the infringement of copyright, even if the manufacturer or seller knows that there is a likelihood that the device will be used for an infringing purpose, so long as the manufacturer or seller has no control over the purchaser's use of that device (see *Australian Tape Manufacturers Association Ltd v Commonwealth* (1993) 177 CLR 480 at 498). Thus, a person does not authorise infringement merely because the person knows that another person might infringe copyright and takes no step to prevent infringement. Mere knowledge 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 infringement (see *Nationwide News Pty Ltd v Copyright Agency Limited* (1996) 65 FCR 399 at 422 and 424).

29 On the other hand, where a website, in substance, constitutes an invitation to use hyperlinks provided on the website in order that sound recordings can be downloaded from other websites and a principal purpose of the first website is to enable infringing copies of the sound recordings to be made, there is an implicit, and possibly an explicit, unqualified invitation to use the website to infringe copyright in the sound recordings. That invitation, when it is taken up, accounts to authorisation (see *Cooper's Case* at [152]).

30 The language of s 112E of the Copyright Act presupposes that a person who merely provides facilities for making a communication might be taken to have authorised an infringement of copyright in a cinematograph film effected by the use of the facility. Absent s 112E, a mere provider of facilities for making communications would be regarded as having authorised copyright infringements effected by the use of those facilities. Section 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 (see *Cooper's Case* at [32] and [39]).

31 Before s 112E will be applicable, there must be a person providing facilities for making or facilitating the making of a communication. However, if the most that can be said is that a person has provided facilities that another person has used to infringe copyright, that first person is not to be taken to have authorised the infringement. Nevertheless, s 112E does not preclude the possibility that a person who attracts the benefit of the section may be held, for other reasons, to be an authoriser. Whether there are other reasons depends on the matters referred to in s 101(1A) and any other relevant matters (see *Cooper's Case* at [168]). Section 112E may provide a defence for a person who does no more than provide the facilities that are used to infringe copyright.

32 It is not necessary, in order to have a relevant power within s 101(1A)(a), that a person must have power, at the time of doing of each relevant act comprised in a copyright, to prevent the act being done. A person's power to prevent the doing of an act comprised in a 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. It is relevant if a person who provides a facility for obtaining access to a website chooses to establish and maintain that facility in a form that does not give that person power immediately to prevent, or immediately to restrict, users of the facility from obtaining access, by means of the facility, to other websites for the purpose of copying material in which copyright subsists. A person has power to prevent the copying of copyright material within the meaning of s 101(1A)(a) if the person is responsible for creating and maintaining a facility whereby the copying can be effected and facilitated (see *Cooper's Case* at [41]-[42]).

33 Indifference, exhibited by acts of commission or omission, may reach a degree from which authorisation or commission may be inferred (*Performing Right Society Limited v Cyril Theatrical Syndicate Limited* (1924) 1 KB 1 at 9). The question is whether the alleged infringer has exhibited such inactivity and indifference as will support a finding of permission. There will be authorisation by a person who decides to ignore the rights of the owner of copyright and to allow a situation to develop and to continue in which the alleged authoriser must have known that the copyright was likely to be infringed (see *Australian Performing Right Association Limited v Jain* (1990) 26 FCR 53 (***Jain***) at 61).

34 While mere inactivity or indifference may be insufficient, particularly where there is no knowledge or reason to suspect that infringement might occur, inactivity or indifference, coupled with other factors, may support an inference of authorisation. It may not be that every act that amounts to the countenancing of something is an authorisation. Matters of degree are involved (see *Cooper's Case* at [38]).

THE TECHNICAL AND FACTUAL BACKGROUND

35 It is necessary to say something about the technical background against which the issues in the appeal arise. It will then be necessary to describe the relevant acts of infringement before describing the extent of iiNet's knowledge of those acts and the action taken by iiNet in response to that knowledge.

The Internet

36 Not every computer using the internet is connected directly to every other computer using the internet. Rather, each computer is linked to other computers, which in turn are

connected to other computers, and so on. Hence, the internet is fairly described as a network of networks of computers.

37 For computers to be able to communicate with each other, they must use the same language. That process is facilitated by sets of rules for computers, which are referred to as **protocols**. Two computers that obey the relevant protocols will be able to communicate with each other. One of the primary protocols by which communication is effected between computers is **the Internet Protocol**.

38 Computers operate by means of binary code. A **bit** is either a zero or a one. A **byte** is 8 bits. A **kilobyte** is 1,024 bytes, a **megabyte** is 1,024 kilobytes and a **gigabyte** is 1,024 megabytes.

39 Data sent by means of the Internet Protocol is broken up into small **packets,** consisting of less that half a megabyte. Each packet contains a header consisting of information identifying the address from which the packet is sent and the address to which the packet is to be sent. The packet itself contains the relevant data. The Internet Protocol allocates addresses to the sending and receiving computers and then sends the packets of data from one address to the other. Such addresses are referred to as **IP Addresses**. An IP Address is a number rendered in binary code. To make an IP Address readable, it is converted into a number consisting of four groups of three digits, each group separated by a full stop.

40 IP Addresses are sold in blocks to carriage service providers such as iiNet, who then allocate them to their customers to enable their customers to connect to the internet and communicate with other computers. The identity of the carriage service provider to which particular IP Addresses have been allocated is public information.

41 Carriage service providers connect their customers to the internet by means of physical infrastructures. The customer's connection to the infrastructure is by way of a modem, which will often be provided to the customer by the carriage service provider. The customer's modem may communicate with the carriage service provider's infrastructure by telephone lines or cables or by wireless transmission. The carriage service provider's infrastructure enables it to communicate with any modem within Australia. iiNet operates

facilities that allow many connections to be aggregated together at an iiNet data centre. iiNet has a connection from its data centre in Sydney to the rest of the world by means of undersea optical fibre cables. By those facilities, iiNet is able to provide connections from each customer's modem to modems of its other customers and of customers of other service providers throughout the world.

42 A **router** is a device that splits the internet connection provided to a particular modem. Splitting the connection will enable two or more computers to have access to the internet by use of the same modem. A router also allows two or more computers to communicate with each other, thereby creating a network. Thus, a single internet connection will be made to a modem. Data passing through that modem will be passed either directly to a single computer or to a router. If to a router then the router will distribute data to the computers that are connected to that router, either by way of a cable or by wireless transmission.

43 Each computer connected to a router is assigned an IP Address by the router in the same form as that used for the internet. However, such IP Addresses are known only to the computers attached to that network and are not publicly available. In particular, the IP Address of a particular computer is not transmitted to the internet. Only the address of the modem is transmitted to the internet. Because all of the computers within a particular network receive data through the relevant router, only one public IP Address is allocated by the carriage service provider to the modem to which the router is connected. The IP Address of the modem, which is public, is the only address seen by other computers on the internet.

44 Thus, the location of a connection to the internet by means of the public IP Address will be known publicly. However, a public IP Address does not necessarily relate to a specific computer but will relate to the modem to which that computer is connected. There may be connected to that modem just one computer or a router to which any number of computers may be connected to form a network. It is only computers within that network, receiving data from the router, that will know the identity of other computers in that network.

45 The IP Addresses provided to most of iiNet's domestic customers for access to the internet are not fixed, but change over time. That is to say domestic IP Addresses are

described as being **dynamic**. On the other hand, business customers are mostly provided with a fixed or **static** IP Address.

The BitTorrent System

46 There are various schemes operating on the internet for the decentralised distribution of data across the internet, usually described as **file sharing**. One of those schemes is **the BitTorrent System**. The BitTorrent System operates on a **peer to peer basis**, whereby all of the computers seeking particular data participate in the distribution of that data. . A group of computers sharing a particular file is known as a **swarm**. Each computer within a swarm is known as a **peer**.

47 The BitTorrent System has a number of constituent parts. The constituent parts of the BitTorrent System include the BitTorrent Protocol, the BitTorrent Client software and the Tracker. Those constituent parts work together to enable access to the ultimate file sought to be shared. In the present context, the file to be shared will be one of the Films.

48 The **BitTorrent Protocol** specifies what needs to be done to implement file sharing by means of the BitTorrent System. A **file extension** specifies the particular purpose of a particular file. The BitTorrent Protocol uses a **.torrent** file extension. A .torrent file does not contain underlying data. Rather it contains the name of a file of interest, the size of the file and other information relating to the data in question

49 **BitTorrent Client** software is a computer programme that allows a person to access groups of computers sharing a particular .torrent file. There are several BitTorrent Client programmes available. Different programmes may have different graphic user interfaces and have different features. However, each BitTorrent Client programme operates in the same basic way insofar as it must comply with the requirements of the BitTorrent Protocol in order to function. In order to fulfil its role, BitTorrent Client must be provided with information from a .torrent file.

50 The BitTorrent Protocol breaks up large files into smaller pieces, in a way similar to that in which data is transferred across the internet by means of packets. The size of the pieces into which the BitTorrent Protocol breaks a file varies. Cinematograph film files are

often divided into pieces consisting of 512 kilobytes. Such pieces will usually be larger than packets.

51 The pieces into which the BitTorrent Protocol breaks up files are shared between the individual peers in a swarm. Over time, pieces are requested and received by the BitTorrent Client programme from other peers and are ultimately assembled together into a file that consists of the whole of the original file. In order to ensure that each piece is received correctly, and that the data is not corrupted, the BitTorrent Client programme consults hash values for each piece.

52 A **hash value** is a means of converting a large amount of data into a smaller value. It is a mathematical function of its input, in that an identical input equals an identical **hash**. Accordingly, a hash can fulfil the function of an identifier of data. The input comes from the data of the file being shared as a whole or as a piece of that file. The hash value for each piece is referred to as a **piece hash**. A .torrent file contains the details of the piece hashes of all the individual pieces of the file in question.

53 When the BitTorrent Client programme 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 programme 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.

54 A **file hash** is the mathematical function of the data of the underlying file as a whole being shared in a swarm. A particular swarm may be sharing one file or a number of files. 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. The file hash can be used to show that a particular swarm is sharing a particular file, which is a cinematograph film. Any copy of such a file with the same file hash will be the same as any other copy with that file hash.

55 Another constituent part of the BitTorrent System is the **Tracker**, which is a computer programme on a server made available for contact by users by means of a Universal Resource Locater, or web address (**URL**). The URL is found in the .torrent file. The Tracker monitors the particular swarm to which it is attached and monitors the IP Addresses of peers in the swarm. The BitTorrent Client programme, 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 programme. That allows the BitTorrent Client programme to contact those peers directly, by their IP Addresses, and request pieces of the file from them and to share pieces of the file with them.

56 Many websites make .torrent files available for download. Such websites have a search function that enables a search to be made for a particular file. Not all .torrent files relate to copyright material. However, some websites openly offer copyright material, including the Films.

57 Several steps are required to enable a person to obtain access to one of the Films by means of the BitTorrent System. First, it is necessary to download a BitTorrent Client programme. Next, .torrent files related to the Films are downloaded from websites on the internet. The .torrent files are then opened in the BitTorrent Client programme. A connection with the internet must be maintained for so long as it takes to download all of the pieces that make up the .torrent file for the Film. The time necessary for the downloading process will depend upon the size of the Film file, the number of peers in the swarm and the speed of the internet connections of those peers.

58 The BitTorrent System enables efficient distribution of data, because each peer is connected to many other peers, the film file is split into many small pieces and peers download pieces from other peers as well as uploading pieces to other peers. The logic of the BitTorrent Protocol operates so as to ensure that the rarest piece in a swarm is the first to be sought, thereby averaging out the availability of pieces and minimising blockage or bottlenecks, which might occur if there were certain pieces of the Film file requested by many peers.

59 The BitTorrent System can be contrasted with traditional client/server models. With such models, if there are many clients, the server must provide the data to all of the clients. That means that, given a fixed amount of capacity to provide data, the capacity has to be shared among all of the clients seeking the same file. Thus, the more people that seek a particular file, the longer it will take for each person to receive that file. With the BitTorrent

System, the more people wanting a file, and therefore the bigger the swarm, the faster each individual peer receives the file.

60 Where a customer of a carriage service provider seeks to obtain a particular Film file, the customer will first download the .torrent file for that Film. The .torrent file will be opened in the BitTorrent Client programme. Upon opening the file, the BitTorrent Client programme will contact the Tracker, seeking details about the swarm sharing that file, including the IP Addresses of peers in that swarm. Once the BitTorrent Client programme has the addresses, it can contact those peers directly. All of the peers can then communicate directly.

61 The customer seeking the Film file would initially not have any pieces of the Film file but the BitTorrent Client programme will know, because of the .torrent file, all of the pieces it needs to obtain, together with the piece hashes of those pieces. The BitTorrent Client programme will query the peers to which it is connected, in order to ascertain which pieces of the Film file those peers have. Some peers may have the whole of the Film file, in which case all pieces will be available. Other peers may have less than the whole Film file, because they are in the process of downloading. However, those peers will still be able to share the pieces that they have already downloaded.

62 After the Tracker has been interrogated, the BitTorrent Client programme can determine which pieces are the rarest and will therefore request those. Pieces are not downloaded in sequence but the rarest is downloaded first and they are all assembled together later. The BitTorrent Client programme will request a particular piece from another peer who is known to have it. That peer must decide whether or not to share. Generally, the only reason why a peer would refuse to share a piece would be that it has too many other peers connected to it. If the peer decides to share the piece in question, it will transmit the piece to the requesting peer's computer. The BitTorrent Client programme will check the piece by means of the piece hash and, if the check is positive, the piece will be accepted. Once that piece is received, the BitTorrent Client programme can transmit that piece to other peers that request it. The process occurs rapidly, with multiple peers and multiple pieces. It is entirely automatic.

63 Over time, the BitTorrent Client programme will receive all of the pieces, which will be assembled together into the complete Film file. At that point, the customer who has the full Film file will be able to share the whole file with the swarm. The BitTorrent Client programme will share the file with the swarm until such time as that programme is closed on the particular computer or the .torrent file is removed from the programme. If the .torrent file is not removed and the BitTorrent Client programme is reopened, the programme will continue to share the file with the swarm.

Evidence of Primary Infringement

64 The Australian Federation Against Copyright Theft (**AFACT**) is an organisation set up for the purposes of assisting its members in relation to infringement of their copyrights. Its members include all of the Copyright Owners and other companies engaged in the film production industry. The members of AFACT provide funds and determine what investigations and activities will be undertaken by AFACT.

65 From August 2007, AFACT used the services of DtecNet Software APS (**DtecNet**) to collect information concerning alleged copyright infringement by internet users in Australia. Between September 2007 and June 2008, DtecNet investigated 190 Australian service providers in relation to different types of file sharing protocols, including the BitTorrent Protocol. It then narrowed its investigations to the BitTorrent Protocol and targeted four Australian service providers, including iiNet.

66 In June 2008, AFACT instructed DtecNet to prepare reports regarding copyright infringements by customers of iiNet using the BitTorrent System. It did so in the form of spreadsheets, which it provided to AFACT. The data in the spreadsheets recorded infringements in respect of one or more of the Films over a period of time by the use of individual iiNet customer accounts.

67 An employee of DtecNet would identify a .torrent file of interest, based on information supplied by the Copyright Owners or by AFACT. DtecNet would then employ a programme known as DtecNet Agent, which is a BitTorrent Client programme, to open that .torrent file. By doing so, DtecNet Agent, as with any other BitTorrent Client programme, was able to query the Tracker, connect peers to the swarm and download pieces from those

peers. DtecNet Agent employed an IP filter to ensure that it only connected to IP addresses of customers of iiNet. Initially, DtecNet Agent downloaded one complete copy of each of the Films being investigated. DtecNet employees viewed the copy to ensure that it corresponded with one of the Films. That process established that a particular file hash corresponded with one of the Films.

68 DtecNet Agent then reconnected to the IP address of an iiNet customer at whose IP address a copy of the file or parts of the file of that Film had been available and downloaded a piece of that file from that IP address. It then matched the piece downloaded with the piece hash through the hash checking process described above. DtecNet Agent then recorded information referable to the peer from which it had downloaded that piece of the file. DtecNet Agent only downloaded one piece from each IP address and then disconnected from that IP address. DtecNet Agent downloaded a new piece from the same IP address every 24 hours.

69 DtecNet Agent created a running log of every activity, which 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 DtecNet Agent. All the information received by DtecNet Agent was recorded and stored on DtecNet's servers. A DtecNet employee then prepared a report containing some or all of the information recorded by DtecNet Agent and set out that information in spreadsheets, which it provided to AFACT.

iiNet's Arrangements with its Customers

70 The ability of iiNet to derive a profit from its business depends largely upon the control or reduction of variable costs. One of the significant variable costs to iiNet in running its business is the cost of acquiring bandwidth from telecommunication companies so that iiNet can provide internet services to its customers. As a general rule, as usage increases, the cost to iiNet increases. Accordingly, an increase in the average usage is reflected in increased cost in the purchase of bandwidth for subsequent periods. When a customer's usage reaches about 50 percent of the customer's quota, iiNet's margin begins to be eroded by the cost of providing that bandwidth and by other costs.

71 Accordingly, it is in the interests of iiNet to ensure that usage by its customers is low in comparison to the quotas provided for in the plans of those customers. iiNet's costs are reduced and its profits increased if its customers do not use all of the quota allocated to them. iiNet's costs are also reduced if customers do not download data from overseas websites. iiNet says, therefore, that it is not in its interest for customers to download infringing material from overseas websites by use of the BitTorrent System.

72 iiNet provides services to its customers under one or other of its broadband plans. Each broadband plan has a fixed price for a fixed download quota per month. That is to say, a customer on a plan who downloads the whole of the quota allocated to the plan pays the same as a customer on the same plan who downloads none or a small part of the quota. All of the activity by a customer using a service under an internet account, such as viewing a web page, is counted against the quota for that customer's plan.

73 Further, the services provided by iiNet to its customers are used for many functions other than downloading material from websites. For example, services provided by iiNet can be used for email, for social networking, for online media and gaming, for voice over internet protocol and for the operation of virtual private networks. Thus, iiNet customers who have infringed copyright are not necessarily using the iiNet service solely for that purpose. It may be that the infringing acts represent only a very small proportion of the total usage of a service provided to a customer by iiNet. Indeed, there are significant activities of iiNet customers that do not involve any infringement of copyright of the Copyright Owners or of any other copyright.

74 iiNet's customer relationship agreement contains the terms of the arrangement between iiNet and its customer. The customer relationship agreement sets out the standard terms and conditions on which iiNet supplies services and products to its customers. It contains:

- **the general terms**, which apply to all services and to all customers,
- **a service description**, which sets out iiNet's standard service description for each particular service,

- **a pricing schedule**, which specifies iiNet's rate plans, pricing and charges for its service, and
- **a fair use policy**, which applies to particular services and customers.

Clause 1.1 provides that, if there is any inconsistency between any of the terms of the customer relationship agreement, the order of precedence will be the service description, the general terms and the pricing schedule.

75 Clause 1.3 provides that iiNet may need to change the customer relationship agreement from time to time and that that may be done without the agreement of the customer. If iiNet reasonably considers that a change to any term of the customer relationship agreement is likely to benefit the customer, or have a neutral impact on the customer, iiNet is entitled to make the change immediately and is not required to tell the customer. However, if iiNet makes any change that will be detrimental to the customer, iiNet must notify the customer at least 21 working days before the proposed change takes effect. If iiNet makes any change that has more than a minor detrimental impact on the customer, the customer may cancel the service without incurring any charges other than usage based charges incurred up to the date of cancellation.

76 By clause 4.1, the customer must, in using the service, comply with all laws and all directions by any government or statutory body or authority and any reasonable directions by iiNet. Under clause 4.2, the customer must not use, or attempt to use, the customer's service to commit an offence or to infringe another persons rights or for illegal purpose or practices and must not allow anybody else to do so. The customer is responsible for, and must pay for, any use of the service, including where unauthorised use has arisen out of a negligent or wrongful act or omission on the part of the customer.

77 Clause 14.2 provides that iiNet may, without liability, immediately cancel, suspend or restrict the supply of the service to the customer if the customer breaches a material term and that breach is not capable of remedy. In addition, iiNet may also cancel, suspend or restrict the supply of the service if the customer breaches a material term, the breach is capable of remedy and the customer does not remedy the breach within 14 days after iiNet gives notice to the customer requiring the customer to do so. iiNet may also cancel, suspend or restrict the supply of the service if the customer breaches clause 4 or otherwise misuses the service or if

iiNet reasonably suspects fraud or other illegal conduct by the customer, or any other person, in connection with the service.

78 iiNet provides a service, known as **Freezone**, whereby its customers may download or stream licensed material. A large quantity and a wide range of material is available by way of Freezone, including films, sport, television programs, games, music and online radio stations. In order to provide that material, iiNet has entered into arrangements with major suppliers and distributors of licensed material. iiNet customers are also able to download content purchased from the online Apple iTunes store by way of Freezone, as well as rent films from iTunes and watch previews of films online. A large number of iiNet customers use the Freezone service. The customers pay for the downloads and no infringement of copyright is involved.

79 Customers of iiNet automatically receive access to the Freezone service at no additional charge when they enter into a plan with iiNet. Material downloaded or streamed through Freezone is not counted towards the customer's quota. iiNet undertakes a number of steps to encourage its customers to use the Freezone service, by promoting it on its website, through newsletters and by media releases. The Freezone service encourages customers to download and stream material legitimately. That benefits iiNet, the owners of copyright material and customers.

80 Apart from the Freezone service, almost any other activity, including viewing a web page, is counted against a customer's quota. If a customer exceeds the quota, the speed at which that customer can download data is significantly reduced. The purpose of that reduction is to avoid the problem of large unexpected bills for high usage by a customer over quota. Accordingly, there is a strong incentive for customers not to exceed their quotas. However, even if a customer exceeds the quota, and the download speed is reduced, the customer can still download or stream material from the Freezone site at normal speeds.

iiNet's Conduct in Preventing Infringements

81 iiNet points to a number of steps that it says that it has taken in the past to discourage infringing acts by the use of its services as follows: Specifically, iiNet provides its services to its customers on the terms and conditions of the customer relationship agreement, which

requires the customer to comply with all laws, and requires the customer not to use the iiNet service to infringe another persons rights or for illegal purposes or practices. Customer service representatives have, in communications with iiNet customers and other users, communicated iiNet's policy that iiNet does not support the BitTorrent System or other Peer to Peer file sharing protocols.

82 iiNet published a web page that states, amongst other things, that the hosting or posting of illegal copyright material using an iiNet service constitutes a breach of the customer relationship agreement and that such a breach may result in the suspension or termination of service without notice to the customer. The warning refers specifically to clauses 4.1 and 4.2 of the customer relationship agreement.

83 iiNet has provided facilities to Copyright Owners to notify iiNet of allegations of copyright infringement by setting up email addresses for the purpose of receiving emails regarding allegations of copyright infringement, by making available a facsimile number for Copyright Owners to send copyright notifications in accordance with the Copyright Act, by making available a postal address for Copyright Owners to send copyright notifications in accordance with the Copyright Act and by publishing a web page that publishes that email address, that facsimile number and that postal address. iiNet has put in place systems, processes and procedures for receiving and dealing with correspondence regarding alleged copyright infringement sent to those addresses and has not taken any steps to block or restrict Copyright Owners from collecting information about iiNet users and iiNet customers.

84 iiNet provides induction training to new employees, including a session on copyright and related issues and communicates to new employees that iiNet does not condone or support copyright infringement. Further, iiNet provides training to customer service representatives prior to their commencing to work in iiNet's call centres. In addition, iiNet has made available to its staff articles and policies by way of its internal intranet including an article that states that it is very important to determine what customers are downloading.

85 iiNet points to its Freezone service, which provides iiNet customers with financial and other incentives that operate to facilitate and encourage users of the iiNet service to download or stream copyright material legitimately through the Freezone service. iiNet does not impose any quotas, limits or caps on the downloading or streaming of material through the

Freezone service and if an iiNet customer exceeds the monthly quota and the download speed is slowed, Freezone material is still provided at standard speeds. On the other hand, once the customer exceeds the monthly quota, iiNet slows the download speed of a customer's account.

86 iiNet works closely with law enforcement agencies, including the Australian Federal Police and the Australian Security Intelligence Organisation. In response to requests from such agencies, on a daily basis iiNet matches IP Addresses to information about its customers. iiNet's internal procedures ensure that such requests for information comply with necessary statutory provisions. iiNet is reimbursed for complying with such requests for information.

87 From 2007, an organisation called Music Industry Piracy Investigations (**MIPI**) began corresponding with service providers in relation to an industry code of practice that would include a notice and disconnection policy in response to copyright infringement by use of the internet. In April 2007, the Internet Industry Association (**IIA**) wrote to MIPI, to the Australian Recording Industry Association (**ARIA**) and to AFACT, communicating the IIA board's concerns in relation to the proposed notice and disconnection policy.

88 Finally, iiNet participated in the preparation of a submission on internet piracy provided to the Commonwealth Government in April 2008, saying that service providers will, and do, co-operate in any actions taken directly by the owners of copyright against file sharers. The submission said that the service providers do not approve, condone or authorise any person engaging in copyright infringement by any means and that the service providers have repeat infringer policies in place. The submission proposed a streamlined preliminary discovery process in the Federal Court or the Federal Magistrates Court, whereby an application for discovery by the owner of copyright could be made according to a pre-agreed protocol, in return for which the service providers would not oppose such an application. iiNet asserts that none of the proposals in the submission were agreed to.

iiNet's Knowledge of Infringements – the Infringement Notices

89 On 2 May 2008, AFACT wrote to iiNet, saying that AFACT was acting on behalf of approximately 50,000 Australians directly impacted by copyright theft, and that members of

AFACT and their related companies are either the owners or exclusive licensees of copyright in the majority of commercially released motion pictures, including movies and television shows. The letter asserted that there was a significant problem in Australia involving customers of Australian carriage service providers, including iiNet, infringing copyright in motion pictures produced and distributed by members of AFACT. The letter said that such infringements invariably occur through the use of peer to peer services, such as the BitTorrent System.

90 The letter of 2 May 2008 then asserted that iiNet had a significant number of customers who appeared to be engaging in infringing activity by transmitting or downloading in Australia copies of the Films without any licence from the Copyright Owners. The letter suggested that no action was being taken by iiNet to prevent or avoid such infringements taking place, despite iiNet being well placed to do so. The letter asserted that iiNet has the capacity and the contractual right to suspend or terminate the accounts of customers who were infringing the copyright of AFACT's members. The letter also asserted that AFACT's members were concerned by the current level of infringement occurring in Australia and the absence of appropriate and effective measures taken by carriage service providers such as iiNet. The letter invited the managing director of iiNet, Mr Michael Malone, to attend a meeting to discuss specific steps that iiNet might take in order to limit the infringement of copyright by its customers.

91 On 2 July 2008, AFACT wrote again to iiNet. The letter was the first of numerous communications notifying iiNet of particulars of alleged infringements of copyright by its customers (**the Infringement Notices**). In the Infringement Notice of 2 July 2008, AFACT repeated that it was investigating infringements of copyright in movies and television shows in Australia by customers of iiNet through the use of the BitTorrent Protocol and that information had been gathered about numerous such infringements of copyright by customers of iiNet. The letter asserted that those infringements involved the communication to the public of unauthorised copies of motion pictures and television shows, which were shared with other internet users by means of the BitTorrent System.

92 The Infringement Notice of 2 July 2008 asserted that the fact that iiNet customers continue to infringe the copyright of AFACT's members in movies and television shows of

the kind identified in the materials enclosed suggested that iiNet had taken no action to prevent those or similar infringements from taking place. AFACT then asserted that the failure to take any action to prevent infringements of copyright from occurring, in circumstances where iiNet knew that infringements were being committed by its customers, or would have reason to suspect that infringements were occurring, may constitute authorisation of copyright infringement by iiNet.

93 Importantly, a spreadsheet prepared by DtecNet was enclosed with the Infringement Notice of 2 July 2008 containing information of alleged infringing activities of identified iiNet customers that occurred between 23 June 2008 and 29 June 2008. The spreadsheet included the following information:

- The date and time that alleged infringements of copyright took place.
- The IP Address used by the identified iiNet customer at the time of each alleged infringement.
- The motion pictures and television shows in which copyright had allegedly been infringed, including many of the Films.
- The names of the Copyright Owners controlling the rights in the relevant motion pictures and television shows.

A compact disc containing an electronic version of material in the spreadsheet was also enclosed with the Infringement Notice of 2 July 2008.

94 The Infringement Notice of 2 July 2008 also attached extracts from iiNet's standard customer relationship agreement. In particular, attention was drawn to the requirement, in clause 14.2 of the customer relationship agreement, that the customer must not use the service provided by iiNet:

- to commit an offence or to infringe another person's rights,
- for illegal purpose or practices

Reference was also made to clause 4.2, whereby iiNet was authorised to cancel, suspend or restrict the supply of the service to the customer if:

- iiNet reasonably suspected fraud or other illegal conduct by the customer or any other person in connection with the service,
- iiNet was required by law to do so, in order to comply with an order, direction or request of an regulatory authority, an emergency services organisation or any other authority,
- the providing of the service to the customer may be illegal or iiNet anticipates that it may become illegal,
- there was excessive or unusual usage of the service, or
- iiNet was allowed to do so under another provision of the customer relationship agreement.

95 By the Infringement Notice of 2 July 2008, AFACT required iiNet to take action as follows:

- Prevent the iiNet customers identified in the enclosed materials from continuing to infringe copyright in the motion pictures and television shows identified in the materials.
- Take any other action available under iiNet's customer relationship agreement against the identified iiNet customers that was appropriate, having regard to their conduct to date.

AFACT requested iiNet to acknowledge receipt of the Infringement Notice and to confirm when that action had been taken.

96 On 9 July 2008, AFACT sent another Infringement Notice to iiNet in much the same terms as that of 2 July 2008. The Infringement Notice of 9 July 2008 enclosed a spreadsheet containing information relevant to infringing activities between further dates. The same information in relation to those infringements was provided as in the Infringement Notice of 2 July 2008. Further Infringement Notices, with relevant spreadsheets, were sent to iiNet on 16 July 2008 and 23 July 2008.

97 On 25 July 2008, Mr Leroy Parkinson, the credit manager of iiNet, responded to the Infringement Notices received up to that time. The response was by way of email, the language and tone of which can fairly be characterised as dismissive. After acknowledging receipt of the Infringement Notices, Mr Parkinson said that iiNet was very concerned about the allegations and suggested that AFACT promptly direct its allegations to "the appropriate authorities". He then referred to the enclosed spreadsheets containing IP Addresses, dates, time and other details, which, he said, were not explained and some of which iiNet did not understand. Mr Parkinson also said that the Infringement Notices made defective references to "identified iiNet customers", and that none of iiNet's customers had, in fact, been identified. He also said that, in the enclosed spreadsheets, IP Addresses had been provided "as if they were synonymous with persons or legal entities". He said that, on that basis, iiNet was unable to comply with AFACT's requirements in any way. Mr Parkinson then went on to say that, to demonstrate iiNet's support for the elimination of copyright infringement, iiNet had passed the Infringement Notices "to an appropriate law enforcement agency", who was said to be better placed to assist AFACT in pursuing offenders. Mr Parkinson referred to the computer crime squad of the West Australian Police.

98 On 29 July 2008, AFACT wrote to iiNet again, referring to Mr Parkinson's email of 25 July 2008. AFACT's letter said that the Infringement Notices of 2, 9, 16 and 23 July 2008, with the enclosed spreadsheets, had provided iiNet with detailed information regarding infringements. The letter asserted that each IP Address listed in the spreadsheets was referable to a computer and to a customer account at the relevant date and time of the alleged infringements. The letter also said that iiNet had no shortage of technically qualified employees who should have no difficulty understanding the information provided in the spreadsheets. The letter asserted that, based on the information provided, iiNet would be able to identify very quickly the relevant customer accounts at the time the alleged infringements took place.

99 In response, Mr Parkinson sent a further email to AFACT on 12 August 2008. Mr Parkinson's email of 12 August 2008 reiterated that an IP Address, date and time did not identify a person, and asserted that iiNet could not possibly know the identity of the person who was using any given service associated with that IP Address. Mr Parkinson pointed out that the service could be a shared or community terminal, such as at a school, a library, an

internet café or a wi-fi hotspot. He said that it may not be a computer in the sole use of an individual. Mr Parkinson asked who, in any of the material provided, had been identified by AFACT as the person to whom iiNet should direct the allegation of copyright infringement.

100 Mr Parkinson's email of 12 August 2008 went on to say that "the vigilante approach being promoted by AFACT" was rejected by iiNet and that the appropriate authorities for the prosecution of offenders and imposition of penalties were not internet service providers, and not AFACT. Mr Parkinson said that iiNet would not accept "the responsibility of judge and jury in order to impose arbitrary and disproportionate penalties purely on the allegations of AFACT". He went on to point out that iiNet is not a law enforcement agency and that, if AFACT was not willing to invest its own resources to protect its members' rights, using the correct channels available, iiNet was not going to do so. The email ended with an assertion that the Australian legal system provides an "arsenal of remedies to bring proceedings against alleged infringers" and that iiNet could not take any inappropriate action against customers as demanded by AFACT.

101 On 20 August 2008, AFACT replied to Mr Parkinson's email of 12 August 2008. AFACT said that iiNet could have no doubt that identified customers were infringing copyright in motion pictures and television shows and that iiNet could identify the customer accounts in question, based on the information supplied by AFACT. AFACT said that, over a period of seven weeks, there had been over 5,702 separate instances of infringements of copyright notified to iiNet, including significant repeat infringements. The letter asserted that those infringements had taken place over iiNet's network and could only continue to occur as long as iiNet provided access to customers who were engaging in infringing activity. AFACT asserted that, with that information, in addition to other information that iiNet already had, iiNet could take action to prevent the infringements from continuing. It said that iiNet could contact each of its customers, could warn them against infringement and could impose sanctions if they continued to infringe copyright using iiNet's network, despite the warnings. The letter ended with the expression of hope that the position would change and that iiNet would take steps to prevent the infringements by its customers from continuing.

102 On 22 August 2008, AFACT sent another Infringement Notice, in the same terms as the earlier Infringement Notices, enclosing a spreadsheet relating to alleged infringements

between 11 August 2008 and 17 August 2008. That prompted a further email from Mr Parkinson, reiterating that, if AFACT has a complaint of a crime, it should contact a law enforcement agency to pursue the matter.

103 The tone of iiNet's communications was thus less than cooperative and less than frank in the approach demonstrated. While there is a basic truth in the disclaimer contained in Mr Parkinson's communications, the communications fail to grapple with the complaint being made by AFACT. The basic proposition being advanced by iiNet was that it could not identify the particular individual who may have operated a computer that downloaded a particular Film by means of the BitTorrent System. In one sense that, is correct, in that from iiNet's point of view, its customer is the operator of the modem that has an IP Address known to iiNet, albeit that the IP Address is a dynamic one, that changes from time to time. On the other hand, it was within iiNet's capacity to identify which modem was being used for download of a particular Film on any particular occasion. iiNet could identify the customer to whom it has provided that modem.

104 Of course iiNet would have no means of knowing whether the modem was connected to a single computer or whether it was connected to a network of computers by way of a router. In that sense, iiNet could not know that any given individual was operating a particular computer for purposes of downloading Films by means of the BitTorrent System. However, iiNet would certainly be able to identify the customer whose IP Address was being used for the download of any Film identified in the spreadsheets provided to iiNet by AFACT.

105 The accuracy of the data contained in the spreadsheets produced by DtecNet, which were enclosed with the Infringement Notices, was not challenged by iiNet. iiNet accepts that the material supplied to it by AFACT, as explained by evidence from DtecNet before the primary judge, established that iiNet users had made available online to the public 100 percent of certain of the Films. iiNet conceded that thousands of infringements had occurred. However, iiNet's position is that it was not until well after the commencement of the proceeding that it fully understood the information provided to it by AFACT.

106 In the course of discovery in the proceeding, data compiled by DtecNet was provided to iiNet to enable the identification of the accounts of 20 iiNet customers. While the identity

of the customers was not disclosed, it was possible to create a schedule of infringements that occurred in respect of the 20 accounts.

107 One of those 20 accounts (**customer RC-08**) was mentioned in the spreadsheets attached to twelve of the Infringement Notices. The first Infringement Notice that mentioned customer RC-08 was dated 28 November 2008. The Infringement Notice of 28 November 2008 showed that customer RC-08 had shared 100 percent of the Film "Pineapple Express", the copyright of which is owned by one of the Copyright Owners. The Infringement Notice of 12 December 2008 also showed that customer RC-08 had shared 100 percent of "Twenty One" another of the Films. Copyright in that film is also owned by one of the Copyright Owners. Other Infringement Notices disclosed that RC-08 shared 100 percent of "Pineapple Express" on 37 other occasions. Customer RC-08 also shared 100 percent of "Twenty One" on one other occasion.

108 Thus, the twelve Infringement Notices in which reference is made to the account of customer RC-08 disclose that customer RC-08 shared 100 percent of one of the Films on 40 occasions. The dates on which "Pineapple Express" was shared by customer RC-08 were various dates from 20 November 2008 to 1 May 2009. The Film "Twenty One" was shared by customer RC-08 on 3 December 2008 and again on 26 July 2009. Similar information was in evidence in relation to the other 19 of the 20 iiNet customer accounts that were identified. Those accounts were referred to in various Infringement Notices.

109 iiNet accepted that it had general knowledge of copyright infringement committed by its customers or that infringement was likely to occur on its facilities. Mr Malone acknowledged that, after the material contained in the spreadsheets had been explained to him, he knew what was happening and had done so since, at latest, April 2009. The primary judge found that, sometime after the commencement of the proceeding, iiNet gained the relevant level of knowledge that enabled it to become aware of the manner in which the material contained in the spreadsheets had been gathered. There is no challenge to that finding. Mr Malone also accepted that the Infringement Notices were compelling evidence of infringement, sufficiently compelling for him to refer the matter to the police.

110 There can be no doubt that iiNet, whose business is concerned with the facilitation of communication in the online environment, understood that the Infringement Notices were

allegations of infringements of copyright. The question however, is whether, given that knowledge, there were reasonable steps available to iiNet, once it received that knowledge, that would have prevented infringements occurring in the future.

THE CLAIMS OF THE COPYRIGHT OWNERS

111 The Copyright Owners' allegations as to infringement on the part of iiNet, as made in the Further Amended Statement of Claim, filed pursuant leave given on 8 May 2009, may be summarised as follows, the numbering being references to the paragraphs of that pleading:

> 57. From no later than July 2008, iiNet provided internet access services (**the iiNet internet services**) to persons in Australia (**the iiNet customers**), including by means of broadband and digital subscriber line services.
>
> 58. In the course of providing the iiNet internet services, iiNet:
>
> - provided iiNet customers with access to the internet,
> - allocated IP Addresses for use by iiNet customers while accessing the internet,
> - charged iiNet customers an access fee,
> - provided or offered to provide iiNet customers with technical support, and
> - published terms and conditions from time to time purporting to prohibit the use of the iiNet internet services for certain activities that would infringe other persons' rights.
>
> 59. From no later than July 2008, iiNet customers and other persons accessing the internet by means of the iiNet internet services (together **the iiNet users**) have, in Australia, in the course of accessing the internet by means of the iiNet internet services:
>
> - made available online to other persons,
> - electronically transmitted to other persons, and
> - made copies of,

the whole or a substantial part of each of the Films.

60. iiNet users, having made copies of the Films in the manner referred to in paragraph 59, have thereafter made further copies of the Films in physical DVD format or on other physical storage media for the purpose of watching, storing or distributing the Films.

61. The acts of iiNet users referred to in paragraphs 59 and 60 were done without the licence of the Copyright Owners.

62. By reason of the matters referred to in paragraphs 59, 60 and 61, the iiNet users have infringed the copyright of the Copyright Owners in the Films.

63. At all material times, iiNet:

- knew or had reason to suspect that iiNet users engaged in, and were likely to continue to engage in, the acts referred to in paragraphs 59 and 60, in that on sixty three occasions from 2 July 2008 to 14 September 2009, iiNet was notified by Infringement Notices issued by AFACT of the acts of iiNet users that occurred from 23 June 2008 to 6 September 2009,
- took no action in response to the Infringement Notices which identified that iiNet users were engaging in, or continuing to engage in, the acts referred to in paragraphs 59 and 60, in that iiNet did not suspend or terminate the iiNet internet services of any iiNet customers, investigate the activities of any iiNet users, or take any other action in response to the Infringement Notices,
- offered encouragement to iiNet users to engage in, or continue to engage in, acts of the kind referred to in paragraphs 59 and 60, in that iiNet did not suspend or terminate the iiNet internet services by means of which those iiNet users accessed the internet,
- failed to enforce the terms and conditions referred to in paragraph 58 in relation to iiNet users who engaged in, or continue to engage in, the acts referred to in paragraphs 59 and

60, in that iiNet did not warn iiNet customers that if their iiNet internet services were used by them or by other iiNet users for the purposes of engaging in acts of the kind referred to above they would be in breach of clauses 4.1 and 4.2 of the customer relationship agreement,

- iiNet did not disconnect, suspend or terminate the iiNet internet services or accounts of any iiNet customers who were in breach of clauses 4.1 and 4.2 of the customer relationship agreement as a result of such breach (by means of the infringing activities of themselves or other persons using the service, whether permitted or not),
- continued to offer the iiNet internet services to iiNet customers who were engaging in, or continuing to engage in, the acts referred to in paragraphs 59 and 60 or whose iiNet internet services were being used by other iiNet users to do so, and
- through its own inactivity and indifference, permitted a situation to develop and continue where iiNet users engaged in, or continued to engage in, the acts referred to in paragraphs 59 and 60.

64. Further or alternatively, at all material times, iiNet:

(a) had the power to prevent the infringements and the continuing infringements, in that:

- the iiNet internet services were provided to iiNet users using technical facilities of infrastructure controlled by iiNet,
- pursuant to the customer relationship agreement, all IP Addresses provided by iiNet to its customers for their use remained the property of iiNet,
- iiNet had the power to disconnect, terminate or suspend the iiNet internet services used by iiNet users,

- iiNet could have chosen not to provide, or to cease continuing to provide, the iiNet internet services to iiNet users, and
- the Infringement Notices provided iiNet with information that was sufficient to enable iiNet to identify relevant iiNet customers and to contact each of them.

(b) has a direct and commercial relationship with iiNet customers, in that it provided the iiNet services to the iiNet customers pursuant to the terms and conditions of the customer relationship agreement, which included a clause that any use of the service is the responsibility of the iiNet customer and the terms of the customer relationship agreement applied to the iiNet customer and also to anyone else who uses the service, regardless of whether or not the iiNet customer gives that person permission to do so.

(c) knew that iiNet users were, or were likely to be, using the accounts of iiNet customers to engage in the infringing activities identified in the Infringement Notices.

(d) took no steps, and further, took no reasonable steps, to prevent or avoid the infringements from continuing to take place, in that the Infringement Notices provided iiNet with information that was sufficient to enable iiNet to identify relevant iiNet customers and to contact each of them and iiNet could have taken the following steps:

- sending a notice or email to iiNet customers warning them that their iiNet services had been identified as being used to infringe copyright,
- notify iiNet customers that their conduct, or the conduct of users of the account, involved a breach of the customer relationship agreement,
- request that iiNet customers, or other users of the account, cease such conduct,

- warn iiNet customers that, if such conduct continued, their iiNet services would be disconnected, suspended or terminated,
- repeat the above steps and, or
- disconnect, suspend or terminate iiNet customers' services.

65. By reason of the matters alleged above, iiNet has authorised the doing of the acts of iiNet users referred to in paragraphs 59, 60 and 62.

66. The acts of iiNet referred to in paragraph 65 were done without the licence of the Copyright Owners.

67. By reason of the matters referred to in paragraphs 58 to 66, iiNet has infringed the copyright in the Films.

THE ISSUES

112 It is common ground that there have been primary infringements of the copyrights of the Copyright Owners by use by iiNet users of services provided by iiNet. However, there is a dispute as to the number of primary infringements that have occurred. The conclusion in relation to that dispute may be relevant to any limitation on remedies under the Safe Harbour Provisions, in so far as that limitation depends upon repeat infringement.

113 The principal issue in the appeal is whether iiNet authorised the acts that constituted those infringements. However, authorisation cannot be considered in the abstract. Rather, it must be determined in the light of the specific acts that are said to have been authorised. Accordingly, it is desirable to deal with the issues relating to primary infringement before considering the question of authorisation by iiNet.

Primary Infringement

114 It is common ground that there have been primary infringements by making the Films available to the public online. However, there is a dispute as to whether iiNet users electronically transmitted the Films through the use of the BitTorrent System. There is also a dispute as to whether, through the use of the BitTorrent System, any particular iiNet user made Films available online more than once and, if iiNet users electronically transmitted the Films, whether they did so more than once through the use of the BitTorrent System. The

number of infringements may impact on iiNet's reliance on the Safe Harbour Provisions. Further, the scale of infringement may impact on the steps that it would be reasonable for iiNet to take to prevent infringement by iiNet users.

115 The issues as to primary infringement may be formulated as follows:

- Whether any iiNet user infringed the right of communication to the public more than once in relation to any Film by making the Film available online, such that there were numerous specific acts of infringement by that iiNet user or repeated acts of infringement by that iiNet user.
- Whether:
    - the whole or a substantial part of any of the Films was electronically transmitted,
    - that transmission was to the public, and
    - an iiNet user was the maker of the transmission,

  so as to constitute communicating the Film to the public by that iiNet user, and, if so, whether that iiNet user infringed the right of communication to the public more than once in relation to any Film by electronically transmitting the Film, such that there were numerous specific acts of infringement by that iiNet user or repeated acts of infringement by that iiNet user.

Authorisation

116 The principal question in the appeal is whether, within the meaning of s 101(1) of the Copyright Act, iiNet authorised such acts of infringement on the part of iiNet users as may be found to have occurred. If it did not, the appeal must be dismissed. For reasons that will become apparent, however, it may not necessarily follow that that would be an end of disputation between the Copyright Owners and iiNet concerning authorisation.

117 In relation to the question of authorisation, a number of issues arise as follows:

- The extent of iiNet's power to prevent the doing of the acts of infringement by iiNet users.

- The nature of any relationship between iiNet and its customers and between iiNet and iiNet users who are not customers.
- Whether iiNet took any reasonable steps to prevent or avoid the doing of the acts that constituted infringement.
- The extent of iiNet's knowledge of the relevant acts of infringement.
- Whether, in the circumstances, iiNet sanctioned, approved or countenanced the relevant primary acts of infringement.

Part 13 of the Telco Act

118 In considering the question of authorisation, it is necessary to determine whether the Telco Act prohibited iiNet from using information to take steps to prevent infringements, such that iiNet would be taken not to have authorised the relevant acts of infringement. Several issues arise in relation to the operation of the Telco Act as follows:

- Whether relevant information falls within s 276 of the Telco Act, and
- Whether any of the exceptions under ss 279, 280, 289 or 290 of the Telco Act applies to that information.

Section 112E of the Copyright Act

119 If the Court finds that, apart from the operation of s 112E of the Copyright Act, iiNet authorised the relevant acts of infringement on the part of iiNet users, it will then be necessary to consider whether s 112E leads to the conclusion that iiNet did not authorise the relevant acts of infringement.

The Safe Harbour Provisions

120 Finally, if the Court concludes that iiNet has authorised the relevant acts of infringement, and that neither s 112E of the Copyright Act nor the provisions of the Telco Act would affect that outcome, there is a question as to the relief under s 115 of the Copyright Act. If the Safe Harbour Provisions apply, it will be necessary to consider the application of s 116AG(3) and s 116AG(5) of the Copyright Act. Two issues arise in relation to the Safe Harbour Provisions, as follows:

- Whether iiNet had adopted and reasonably implemented a Termination Policy within the meaning of s 116AH(1) of the Copyright Act, and
- Whether, the accounts of iiNet customers that have been used by iiNet users to infringe are "accounts of repeat infringers" within s 116AH(1) of the Copyright Act.

CONCLUSIONS OF THE PRIMARY JUDGE

121 The primary judge concluded that there was no authorisation by iiNet of the acts of infringement that were committed by iiNet users. That was sufficient to dispose of the proceeding. However, his Honour also dealt with the other issues.

Primary Infringement

122 The primary judge concluded that each Film was made available online only once, albeit perhaps for an extended period of time, on occasion not being accessible for periods of time, such as when the iiNet user's computer is turned off. While an iiNet user may make a particular Film available online only once, the exact moment when that occurs will vary on a case by case basis. However, his Honour did not consider that to be an issue. Whatever the frequency of the infringements, there were, as iiNet conceded, many instances of iiNet users making the Films available online, without the licence of the Copyright Owners.

123 The primary judge rejected an approach that focussed on each individual piece of the file transmitted within the swarm as an individual example of an electronic transmission. His Honour observed that the BitTorrent System does not exist outside the aggregate effect of those transmissions, since a peer will seek the whole of a Film file, not a piece of it. His Honour considered that the correct approach is to view the swarm as an entity in itself. The acts of electronic transmission, therefore, occurs between the iiNet user or peer on the one hand and the swarm on the other, not between each individual peer. His Honour accepted that one on one communications between peers is the technical process by which data is transferred. However, his Honour considered that the communication right referred to in s 86(c) does not necessarily focus upon that level of detail. While the DtecNet evidence could not prove directly that an iiNet user had electronically transmitted a Film to the swarm,

his Honour considered that the evidence was sufficient to draw an inference that, in most cases, iiNet users had done so.

124 The primary judge did not consider that **electronically transmit**, in connection with the BitTorrent System, was a series of single acts. Rather, the BitTorrent System is an ongoing process of communication for as long as one wishes to participate. Therefore, his Honour considered, the term electronically transmit could not sensibly be seen as anything other than a single ongoing process, even if the iiNet user transmits more than 100 per cent of the Film back to the swarm. Once it is accepted that 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, his Honour concluded, each iiNet user electronically transmits each Film only once.

125 The primary judge concluded that the person responsible for determining the content of the communication is the iiNet user who chooses a particular .torrent file, connects to the swarm and, over time, electronically transmits, to that swarm, the file and the pieces that are received. His Honour considered that the effect of s 22(6A) was that the iiNet user did not electronically transmit if the iiNet user receives data from the swarm. His Honour considered, rather, that the electronic transmission is **from** the iiNet user **to** the swarm. His Honour considered that the DtecNet evidence, coupled with the evidence as to the operation of the BitTorrent System, gave rise to an inference that there was an electronic transmission by iiNet users to the swarm and that such transmission infringed the copyright owned by the Copyright Owners.

Authorisation

126 The structure of the reasons of the primary judge in dealing with authorisation under s 101(1A) may be thought to be unconventional. The reasons begin with a consideration of a number of judicial decisions dealing with authorisation prior to the enactment of s 101(1A) and conclude that iiNet did not provide **the means** of infringement, in the relevant sense used in *Moorhouse*, in that it did not extend an invitation to the iiNet users to use its facilities to do acts comprised in the copyright of the Copyright Owners. Consequently, his Honour found, iiNet did not authorise the acts of infringement of copyright done by the iiNet users. His Honour then observed that s 101(1A) was meant to elucidate, not vary, the pre-existing law

of authorisation, but said that he would find that iiNet did not authorise the infringement by iiNet users, regardless of any consideration of s 101(1A). Nevertheless, his Honour accepted that he was compelled to undertake further consideration of the issue of authorisation, including the three matters referred to in s 101(1A). If his Honour accepted that he was compelled to consider the three matters referred to in s 101(1A), it might be expected that his Honour would have considered those matters before reaching a conclusion that there had been no authorisation by iiNet.

127 The primary judge concluded that it would not be reasonable for iiNet to suspend or terminate a customer's account and that, for the purposes of s 101(1A)(a), iiNet, therefore, had no relevant power to prevent the acts of infringements that were occurring. It followed from making that finding, his Honour said, that the claim that iiNet had authorised the infringements on the part of the iiNet users must fail. After considering the relationship between iiNet and the iiNet customers, for the purposes of s 101(1A)(b), his Honour concluded that, while there is a relationship between them, such relationship of itself did not persuade him that iiNet was authorising the acts of infringement by the iiNet users. His Honour concluded that the only relevant power to prevent infringement was a scheme of notifying and then terminating or suspending customer accounts but that he had already found that such a step was not a reasonable step for the purposes of s 101(1A)(c).

128 The primary judge observed that s 101(1A) was not intended to prevent the Court from considering matters other than those mentioned in s 101(1A)(a), s 101(1A)(b) and s 101(1A)(c) when considering whether authorisation of infringement was made out. His Honour then considered three other matters:

- iiNet's knowledge of infringements,
- Encouragement of infringements by iiNet, and
- Inactivity or indifference in relation to the infringements on the part of iiNet.

Finally, his Honour considered whether iiNet had sanctioned, approved, or countenanced the acts of infringement by iiNet users, on the basis that those three words were synonyms of authorise, when used in s 101(1).

129 The primary judge concluded that iiNet had knowledge of the infringements that were occurring and that it would be possible for iiNet to stop the infringements occurring. However, his Honour found, as a matter of fact, that iiNet did not authorise the infringements. That finding was premised on the fact that iiNet did not provide **the means** by which the iiNet users infringed. His Honour also found that, even if that first finding be wrong, while iiNet could stop the infringements occurring in an absolute sense, the steps to do so were not a power to prevent the infringement or a reasonable step in the sense used in s 101(1A)(a) or s 101(1A)(c). Finally, his Honour found that iiNet did not approve, sanction or countenance the acts of infringement by iiNet users. Accordingly, his Honour found that the proceeding against iiNet must fail.

130 The primary judge drew a distinction between the provision of a **necessary precondition to infringement** and the provision of the **actual means of infringement**. His Honour accepted that the provision by iiNet of access to the internet was a necessary precondition for the infringements by iiNet users that occurred. However, his Honour considered that that did not mean that the provision of the internet was provision of **the means** of infringement, since there are also other necessary preconditions of infringement, such as the computers upon which the infringements occurred or the operating systems of those computers.

131 The primary judge considered that the use of the BitTorrent System as a whole was not just a precondition to infringement but was, in a very real sense, **the means** by which copyright was infringed by iiNet users. There was no evidence of infringement occurring, other than by the use of the BitTorrent System, and iiNet users could not have infringed copyright in the way they did from the **mere** use of the services provided by iiNet in providing access to the internet. Rather, there must always be an additional tool employed. Absent the BitTorrent System, the infringements that occurred could not have occurred. His Honour concluded, therefore, that it was not something provided by iiNet, but the use of the BitTorrent System as a whole, that was **the means** by which copyright was infringed by iiNet users and that the provision by iiNet of its internet service did not, by itself, result in the infringements in question.

132 The primary judge expressly declined to find that any constituent part of the BitTorrent System was the **precise** means of infringement. His Honour did not consider that the BitTorrent System could sensibly be seen as anything other than all the constituent parts of that system working together. However, iiNet had no dealings with any organisation that produces any part of the BitTorrent System and there was no connection whatsoever between iiNet and any part of the BitTorrent System.

133 The primary judge therefore concluded that iiNet did not provide **the means** of the infringements in question, in that it did not extend an invitation to its customers or to iiNet users to use its service to do acts comprised in the copyrights of the Copyright Owners. Accordingly, his Honour concluded, iiNet did not authorise the acts of infringement of copyright done by iiNet users.

The Telco Act

134 The primary judge concluded that disclosure or use of the AFACT information, the Score information or the Rumba information would be prohibited by s 276 of the Telco Act, but for the exceptions found in s 289 and s 279 of the Telco Act. Accordingly, his Honour concluded that the defence based on the Telco Act raised by iiNet did not mean that warning, termination or suspension of an iiNet customer's account, based on the information found in the Infringement Notices, was not a relevant power that could be exercised to prevent infringement.

Section 112E

135 While the primary judge found that iiNet had, at some point, knowledge sufficient to act, in relation to the accounts of iiNet customers his Honour did not consider that that would lead to the conclusion that iiNet authorised the relevant acts of infringement. Nevertheless, his Honour concluded that, if it did, s 112E would not afford any protection to iiNet. His Honour considered that, so long as an alleged authoriser has knowledge of the infringements, s 112E will not have any operation.

The Safe Harbour Provisions

136 In relation to the Safe Harbour Provisions, the primary judge considered that iiNet's notification that copyright infringement may lead to termination of customers' accounts was sufficient to put iiNet users on notice that iiNet had a policy in relation to repeat copyright infringement. His Honour considered that Mr Malone's understanding of the factors necessary to take action under that policy was sufficient to constitute a repeat infringer policy for the purposes of condition 1 of item 1 of s 116AH(1). Further, His Honour concluded that iiNet had reasonably implemented that repeat infringer policy. While iiNet's requirement that an iiNet user be found to have repeatedly infringed copyright by a court set a high bar before iiNet would effect termination of the account being used by an iiNet user, his Honour concluded that, in the circumstances of category A activities, the policy was an appropriate one. His Honour therefore concluded that iiNet had adopted and reasonably implemented a repeat infringer policy and, accordingly, satisfied the requirements of the Safe Harbour Provisions. Therefore, his Honour considered, the orders that the Court would make would be limited to those found in s 116AG(3) of the Copyright Act. However, having regard to the conclusions reached by his Honour in relation to authorisation, it was not necessary to consider any remedies.

INTERVENTION BY OTHER PARTIES

137 Prior to the hearing of the appeal, two applications were made for leave to intervene to make submissions on the hearing of the appeal. One application was made by Australian Performing Right Association Limited (**APRA**). The second application was a joint application by the Media Entertainment and Arts Alliance (**MEAA**) and the Screen Actors Guild (**the Guild**). The applications were made under Order 52 Rule 14AA of the Federal Court Rules. Both applications were opposed by iiNet. The Copyright Owners did not oppose the applications.

138 Under Order 52 Rule 14AA(1), the Court may give leave to a person to intervene in an appeal on such terms and conditions, and with such rights, privileges and liabilities, including liabilities for costs, as the Court may determine. Under rule 14AA(2), in deciding whether to give leave, the Court must have regard to:

- whether the proposed intervener's contribution will be useful and different from the contribution of the parties to the appeal,
- whether the intervention might unreasonably interfere with the ability of the parties to conduct the appeal as they wish, and
- any other matter that the Court considers relevant.

The role of the intervener is solely to assist the Court in its task of resolving the issues raised by the parties to the appeal.

139 Rule 14AA is intended to regulate comprehensively the Court's practice with respect to the intervention of non parties (see *Sharman Networks Ltd v Universal Music Australia Pty Ltd* (2006) 155 FCR 291 at [11]). Where the parties to an appeal are represented by substantial and competent teams of lawyers and an applicant for leave to intervene proposes to raise matters already ventilated by the parties to the appeal, the application for leave to intervene would normally be refused (see *ASIC v Citigroup Global Markets Australia Pty Limited* (No.3) [2007] FCA 393 at [12]-[13] and *Levy v State of Victoria* (1997) 189 CLR 579 at 604).

Application by APRA

140 APRA is a not for profit collecting society under the Copyright Act. Its function includes enforcing copyrights assigned to it by its members. APRA owns, or represents the owners of, the exclusive right under s 31(1)(a)(iv) of the Copyright Act to communicate relevant works to the public throughout Australia. APRA's interest in the outcome of the appeal is aligned with the Copyright Owners. However, APRA contends that it has an interest different from that of the Copyright Owners, although it concedes that there is overlap between the submissions of the Copyright Owners and the submissions that APRA wishes to make.

141 APRA sought leave to make submissions on three related legal questions as follows:

- A distinction adopted by the primary judge between two different classes of cases described as the **APRA cases** and the **technology cases**,

- The focus of the primary judge on identifying the means of infringement, which APRA contended is contrary to the Copyright Act and is apt to lead to error, and
- The proper role of s 101(1A).

APRA did not seek to make submissions as to the application in the present appeal of the principles that it proposed to propound.

Application by MEAA and the Guild

142 MEAA is a union and professional association for those involved in the media, entertainment, sports and arts industries. It was formed in 1992 by the merger of trade unions covering the interests of actors, journalists and entertainment industry employees. Other organisations have joined MEAA since that merger. More than a third of MEAA's members are actors or other performers engaged or potentially engaged in making films and television productions. About 95% of performers in Australian films and television productions are members of MEAA.

143 The Guild is the largest labour union representing working actors in the United States of America. The Guild was established in 1933 and represents over 125,000 actors who work in the film and television industries, commercials, video games, music videos and other media formats. The Guild exists to enhance actors' working conditions, compensations and benefits and to be a voice on behalf of the rights of artists.

144 MEAA and the Guild together have as members, and represent the professional interests of, almost all Australian and United States performers in films and television productions. The application to intervene is made on behalf of members engaged in the film and television industry, particularly as performers.

145 MEAA and the Guild propounded submissions in support of the Copyright Owners' position. They sought to address two aspects of the appeal that, they say, might otherwise be overlooked or be given insufficient emphasis because they affect more directly the interest of performers in films and television productions than the interest of the Copyright Owners. The aspects sought to be addressed may be summarised as follows:

- The approach taken by the primary judge as to the meaning of **make available online** and **electronically transmit**, which may affect the value of residual rights, such as the sale of authorised copies of films and television productions on the basis of which performers are often renumerated.

- The considerations raised by references in s 101(1A) to **reasonable steps** and in s 116AH to **appropriate circumstances**, being considerations based on limited financial resources and lack of access to expert legal advice, which would not be central to the contentions of the Copyright Owners but may be of significance to members of MEAA and the Guild.

Whether intervention should be permitted

146 At a directions hearing prior to the hearing of the appeal, the parties indicated that they were content for the question of intervention to be determined at the hearing of the appeal. Hence, the applicants for leave were directed to file and serve the detailed written submissions that they would wish to make if leave were granted. In a sense, that course pre-empted the question of leave. Nevertheless, the direction was given without opposition and was appropriate in order to make clear the scope of the contribution that might be made by the interveners and the possible interference with the conduct of the appeal. At the hearing of the appeal, the interveners were given the opportunity to make brief oral submissions in support of their written submissions. The Court reserved the question of whether formal leave would be granted.

147 In all of the circumstances, it is appropriate to give leave to both APRA and to MEAA and the Guild to make the submissions that they have in fact made. Their submissions may afford some assistance and place emphasis on matters beyond the matters addressed by the Copyright Owners. iiNet has had ample opportunity to deal with the submissions, which have not interferred with the ability of iiNet or the Copyright Owners to conduct the appeal. Neither the written submissions nor the oral submissions made by the interveners have added materially to the costs of the appeal. There should be no order as to the costs of the applications.

148 To the extent that they have a bearing on the outcome of the appeal, the substance of the submissions has been dealt with in the relevant parts of the reasons. Not all of the submissions made by the interveners are necessarily relevant.

PRIMARY INFRINGEMENT

149 iiNet accepted that iiNet users who had shared 100 percent of a Film infringed copyright in the Film by reproducing the Film on the computer used by that iiNet user. iiNet also accepted that each such iiNet user had also infringed copyright in that Film by communicating it to the public within the meaning of s 86 of the Copyright Act.

150 The issue in relation to primary infringement is whether there were repeated acts of infringement by individual iiNet users. That question turns on the proper construction of the words **make available online** in the definition of **communicate** in s 10 of the Copyright Act and whether an iiNet user who participates in the BitTorrent System makes a Film available online to the public once or multiple times. Another question is whether there were also acts of infringement by electronically transmitting Films to the public, and if so, whether there were multiple infringements by individual iiNet users.

Making Available Online

151 iiNet says that **making available online**, in s 86 of the Copyright Act, refers to something done by a human act, not by the operation of a computer. The act of making something available, iiNet says, can only sensibly be done once, by a human user, when the sequence of actions is taken to download a file and leave it available to the BitTorrent Client programme, which allows the file to be made available to other persons, being members of the swarm. It says that it is an artificial straining of the language of s 86 to say that such an act is renewed artificially, for example, by switching on or off a computer or the dropping in or out of connection to the internet. iiNet contends that, when a user of the internet searches for a .torrent file and evokes that .torrent file in the BitTorrent Client programme, so as to download one of the Films, with the result that 100 percent of that Film is copied to that user's hard drive and, by reason of the BitTorrent Protocol, is made available online, that amounts to the doing of one infringing communication and one infringing copying by that user.

152 Those contentions must be rejected. There is nothing in the Copyright Act to suggest that successive connections of a modem to the internet should be deemed to be but one event. Connection to the internet is an essential element in making available online, in that communication cannot occur if there is no connection to the internet. Where a particular modem is not connected to the internet, that modem could not be making a Film available online. Every time that a modem is connected to the internet, and makes a Film available, there is a new making of the film available online. A separate act is engaged in each time a modem is connected to the internet and goes online. A computer must connect to the modem, or to a router attached to the modem, and, in the case of a non-business account of iiNet, is then allocated a dynamic IP address. Where the connection is severed, the computer or modem is no longer associated with that dynamic IP address. To reconnect to the internet, there must again be a contact with the modem to which an iiNet service is provided and a new IP address is allocated. There must be intervention by a user for each of those steps.

153 If a user connects to the internet on multiple occasions, as in the case of the user of the account of customer RC-08, multiple acts are involved. The connection history of customer RC-08 demonstrates that users of the account of customer RC-08 disconnected from the internet from time to time and sometimes did not reconnect for hours or days. Users of the account of customer RC-08 must, in those circumstances, have taken steps to end each internet connection. While there was no evidence as to the reason for any given termination of the connection, the reason for termination is irrelevant. Each new connection gives rise to a new session of being online.

154 Where an iiNet user downloads or installs a BitTorrent Client Programme on a computer, that iiNet user must have made a conscious decision to enable the relevant computer to participate in the BitTorrent System. When an iiNet user switches on that iiNet user's computer and connects it to the internet, through a modem using the service provided by iiNet, the iiNet user must be taken to have intended that the BitTorrent System would operate in accordance with the BitTorrent Protocol. Each time that the computer is connected to the internet, and is capable of participating in the BitTorrent System, any Film file stored in that computer is made available online for other members of the swarm, namely, those other computer operators who are participating in the BitTorrent System by having a BitTorrent Client Programme operating on their respective computers. From the point of

view of an iiNet user whose computer participates in the BitTorrent System, every time the computer is connected to the internet, all files relating to a Film will be made available to be uploaded, albeit in pieces, by means of the BitTorrent System, using the BitTorrent Client Programme on the computer, as well as the Tracker and the BitTorrent Protocol. Transmission cannot occur when there is no connection to the internet.

155 The accuracy of the data contained in the spreadsheets produced by DtecNet, which were enclosed with the Infringement Notices, was not challenged by iiNet and iiNet conceded that thousands of infringements had occurred. The data in the spreadsheets recorded infringements in respect of one of the Films or more than one of the Films over a period of time by the use of individual iiNet customer accounts. The spreadsheets collated data by reference to the Peer ID. Where DtecNet Agent downloaded two or more pieces of a Film from the same Peer ID, those pieces emanated from the same computer and were initiated by the same person.

156 iiNet also contends that no inference should be drawn that a single person was involved in relation to all the infringements in connection with the account of customer RC-08. There was unchallenged evidence of individual iiNet accounts being involved in dealings in more than one of the Films at once. However, iiNet does not dispute that an inference might be drawn that at least some of its customer accounts are used by one person only.

157 The infringement in question is an infringement by the iiNet customer whose account is being used. An iiNet customer whose account is being used to make Films available online cannot deny responsibility for the way in which the iiNet service is used. The iiNet customer must accept responsibility for the way in which the service provided by iiNet to that customer is used. Infringement by an iiNet user of a computer attached, by means of a router or otherwise, to a modem to which an iiNet service is provided, is a use of the service provided by iiNet to that modem. An iiNet customer is infringing by permitting the use of the service for infringement.

158 It follows that those iiNet users who utilised the account of customer RC-08, repeatedly made available online the Film Pineapple Express and also made available online the Film Twenty One at least twice. The accounts of many iiNet customers were identified as

making available online more than one of the Films, as with customer RC-08. That constitutes a repeat infringement.

Electronic Transmission

159 The Copyright Owners contend that, by reason of the manner in which the BitTorrent System operates, there were electronic transmissions between the iiNet users identified by DtecNet Agent and the aggregate of the peers who constituted the BitTorrent swarm. Unlike the traditional client/server model, the BitTorrent System operates, not by one on one communication, but by a multitude of communications between a multitude of computers. It works by transmitting thousands of pieces to hundreds of different peers, even though the underlying technical process involves communications directly between one peer and another. However, the Copyright Owners contend that the proper approach for the purposes of the Copyright Act requires identification of a transmission as occurring between the iiNet user, or peer, and the swarm. It does not involve identification of a transmission between each individual peer.

160 The Copyright Owners say that the DtecNet peer computers that recorded the transmissions taking place were representative of the computers that were in the swarm and that the evidence provided a sufficient foundation for an inference that there had been electronic transmissions of the whole or a substantial part of the Films to the swarm. They contend that the DtecNet evidence supports a finding that, in most cases, iiNet users had electronically transmitted a Film file to the swarm.

161 iiNet contends that, because the BitTorrent System does not use a traditional client/server model to provide data to clients, but rather involves a multitude of communications between a multitude of computers, whereby data is sourced from many different peers in the swarm, the notions of electronic transmission of a substantial part of a Film are difficult to apply. iiNet says that the BitTorrent System operates by transmitting thousands of pieces of a Film to many different peers. Each piece is highly unlikely to be a substantial part. Thus, a person downloading a Film by means of the BitTorrent System obtains the many pieces of the relevant Film from various other peers, who may be from all over the world. Each particular piece is shared in a direct transaction between the peer processing the piece and the peer seeking the piece. iiNet contends that a one on one, or peer

to peer, communication in those circumstances is not a communication to the public within the meaning of s 86(c) of the Copyright Act.

162 The effect of s 14 of the Copyright Act is that if an act is done in relation to less than the whole of a work or other subject matter in which copyright subsists, there is no infringement unless a substantial part is involved. A feature of the BitTorrent System is that pieces obtained by a downloader are only fragments of the whole Film. iiNet says that, in those circumstances, where only small, if regular, helpings are taken, there is no infringement (see *IceTV Pty Limited v Nine Network Australia Pty Limited* (2009) 239 CLR 458 at [21]). iiNet says that, before there will be infringement in those circumstances, the whole or a substantial part of the relevant subject matter must be transmitted by someone. That requires discrimination between members of the swarm who are iiNet users and those who are not. It must also involve discriminating between users in Australia and users who are not in Australia. iiNet contends that, once it is accepted that an iiNet user might obtain the whole of a Film by downloading, without sharing the same amount of data back into the swarm, it is not permissible to assume that, because the viability of swarms in a general sense relies on peers providing at least as much data as they take, the individual iiNet users detected sharing a single piece of a Film in fact had shared a substantial part of that Film. iiNet says that there is no evidence in relation to any one act of transmission caused by individual DtecNet interrogations of individual iiNet users that constituted sufficient acts of transmission by the same user, being an iiNet user located in Australia, whereby a substantial part of any particular Film was transmitted.

163 The Copyright Owners answer that proposition by saying that, since it is in the nature of the internet that the transmission of data is effected by means of that data being broken up into a multitude of packets, to focus on an individual packet would render it impossible for an electronic transmission, in the sense contemplated by s 86(c), to occur in any circumstances. The Copyright Owners say that the relevant transmissions were between an iiNet user and the swarm and that satisfies the requirement that there be an electronic transmission of Films to the public.

164 The width of the statutory definition of communicate in s 10(1) of the Copyright Act, and the extrinsic material relating to the Digital Agenda Act, make it plain that the

introduction of the right of communication **to the public** was intended to provide a technologically neutral right to cover technological developments such as the internet. The DtecNet evidence was that a filter was applied to restrict connections only to other iiNet users. In those circumstances, the exchange of Film files between the users indicated that substantial parts of the Film files were being transmitted and received between them.

165 The Copyright Owners contend that the question of whether electronic transmissions were relevantly to the public does not depend upon whether the transmissions are between the iiNet user and the swarm or the iiNet user and other internet users. In both cases, they say, the transmissions are to the public. The relevant relationship is the potential commercial relationship between the owner of copyright and an infringer, not between infringers engaged in file sharing. There is a potential commercial relationship between the Copyright Owners and infringing iiNet users in the present case, given the range of legitimate avenues available for the transmission of Films through sources such as iTunes. The illegitimate transmission of Films over the internet reduces such commercial opportunities and deprives the Copyright Owners of revenues to which they would be entitled as the owners of copyright.

166 Section 22(6) provides that the maker of a communication is the person responsible for determining the content of the communication. Section 22(6A) has the effect that a person is not responsible for determining the content of a communication merely because the person takes a step to gain access to what is made available online or to receive an electronic transmission. It is not correct to say that the sole causative factor in the transmission taking place and the content of the transmission is the request from the downloading computer. The process of electronic transmission is not simply one of a request and transmission, determined by the requesting party. The sender of the Film file is the party who determines the content of the communication, by having the BitTorrent Client software installed in a computer so as to respond to a request for a Film file, thus permitting the communication to occur.

167 iiNet contends that the only direct evidence is that DtecNet recorded the receipt from various iiNet users of a single piece of a Film. It says that the question is not answered by acknowledging that the BitTorrent System, as a whole, depends on the exchange of the whole of a Film or individual users sending as well as receiving files. There must be an act of primary infringement before iiNet can be said to have authorised it. Thus, iiNet says, the

Copyright Owners must establish that there was done, in Australia by an iiNet user, an act comprised in the copyright, relevantly a transmission of the whole or a substantial part of one of the Films. It says that the evidence and the inferences available from the evidence do not support such a conclusion.

168 iiNet accepts that, if a person attached an infringing copy of a Film to an email and sent it by means of the internet to a recipient, there would be an electronic transmission of the whole of the work, notwithstanding that the work would be divided into a multitude of packets in accordance with the ordinary operation of the internet. iiNet says that there is no evidence that a recipient under the BitTorrent System would receive the whole or a substantial part of one of the Films from an individual iiNet user. iiNet says that the very essence of the swarm, being comprised of many users from all around the world, means that it is very unlikely that somebody would receive the whole or a substantial part of one of the Films from an individual iiNet user.

169 As iiNet says, the object of the Digital Agenda Act, to create a technology neutral right of communication, cannot override the plain words of the Copyright Act itself. There must be an electronic transmission by a user in Australia of a whole or substantial part of relevant subject matter in which copyright subsists, such as a Film. iiNet concedes that there has been communication by making available. Accordingly, the communication right has attached to acts of iiNet users that employ the BitTorrent System. iiNet contends, however, that it does not follow that the communication right attaches to all such conduct or that every limb of the communication right must be engaged.

170 The evidence of the DtecNet spreadsheets is such that it is very difficult to reach a conclusion on the question of whether iiNet users have electronically transmitted a substantial part of any of the Films to the public. Having regard to the conclusion reached above, that there are multiple repeat infringements by iiNet users making Films available to the public online, it is not necessary to resolve the question finally.

AUTHORISATION

171 In the light of s 101(1A) and *Moorhouse*, the appropriate approach to determining whether acts of infringement have been authorised, is, first, to identify the acts that constitute

infringement of copyright. It is then necessary to identify what was done by the alleged authoriser in relation to those acts of infringement. Next, each of the three matters referred to in s 101(1A) must be considered, together with any other relevant matters. It is then necessary to consider the s 112E and Telco Act defences.

172 In the present context, the acts of infringement alleged to have been authorised were making the Films available to the public online, as described above. The conduct of iiNet was the provision to its customers, under its customer service agreement, of services by use of which such communications were made, in the circumstances described above. It is therefore necessary to deal with s 101(1A) and the other considerations relevant to authorisation. I shall then deal with the s 112E and Telco Act defence.

Authorisation Under s 101

173 A person will authorise an act of infringement if the person sanctions, approves or countenances the act. Those words should be understood disjunctively not conjunctively. Countenancing does not mean the same thing as approving and includes turning a blind eye and tolerating or permitting. The question is whether iiNet tolerated and permitted acts of infringement to continue.

174 iiNet was aware that allegations were being made that infringements by users of its services had occurred. To the extent that it could rely on the information provided by the Infringement Notices, it was in a position to determine the identity of the customers whose accounts were involved in the infringements. iiNet had the power to prevent further infringements involving those accounts by suspending or terminating the accounts. That is to say, iiNet was in a contractual and technical relationship with customers whose accounts were involved in infringements whereby:

- iiNet contracted to provide and did in fact provide the necessary facilities,
- iiNet's customers undertook not to infringe copyright,
- iiNet reserved to itself the right to take action, including suspending or terminating services, if its customers infringed copyright, and
- iiNet benefited financially from continued usage of its services.

However, iiNet took no step to suspend or terminate any account in order to prevent or avoid the making of the communications that constituted subsequent infringements.

175 iiNet derived a financial benefit from the continuation of its relationship with its customers. Were iiNet to have acted on any of the Infringement Notices and taken steps to warn a customer and then suspend or terminate an account, iiNet ran the risk of suffering the commercial impact of the loss of such customers to other service providers.

176 iiNet adopted the position that acts of infringement, by use of its customers' accounts, were not its problem and that it would do nothing more to prevent such acts recurring. That is to say, iiNet was content to do nothing to prevent alleged acts of infringement continuing to occur. iiNet was concerned about the potential for antagonising its customers, which might lead to their entering into arrangements with other service providers. Therefore, it sought to assure its customers that it would not act on the Infringement Notices. That conduct is capable of constituting at least tacit approval.

177 iiNet contends that it did not authorise any act of infringement by any of its customers because no express authority or invitation to do such acts was conveyed by iiNet to any of its customers. Further, it says, no implied authority or invitation was conveyed because:

- iiNet's customer relationship agreement with its customers exacted a promise from each customer not to engage in acts of infringement by use of the iiNet service,
- iiNet published a warning to that effect on the copyright page of its website,
- iiNet publicly promoted the licensed distribution of copyright material and encouraged its customers to obtain licensed copyright material, by use of the Freezone service,
- iiNet customers accused by the Copyright Owners of engaging in acts of infringement did not know that they had been detected and, accordingly, they could not regard continued access to the internet by means of the iiNet service as a sign of approval or countenancing of the conduct by iiNet,
- iiNet did not provide iiNet users with the BitTorrent Client programme, without which the acts of infringement complained of could not be done,

- iiNet did not provide iiNet users with the copyright material that was infringed,
- iiNet's only relevant power to prevent future acts of infringement was to disconnect its customers in respect of whose accounts allegations had been made and that was not a reasonable step,
- iiNet's decision not to notify its customers of allegations of copyright infringement, and thereafter disconnect the customer, was not unreasonable having regard to the cost and complexity of doing so and the disproportionate nature of such a response,
- The actual acts of infringement may have been done by an iiNet user other than the actual iiNet customer.

Section 101(1A)

178 Each of the three matters referred to in s 101(1A)(a), s 101(1A)(b) and s 101(1A)(c) must be taken into account in determining whether or not a person has authorised the doing of an act comprised in a copyright. However, each paragraph must be understood in its context.

179 The language of s 101(1A)(c) is curious in that it refers to any **other** reasonable steps. On one view, the word **other** adds nothing because the matters referred to in s 101(1A)(a) and s 101(1A)(b) are not steps. However, the language of s 101(1A)(c) does not warrant reading into s 101(1A)(a) a qualification that is only **reasonable** power that must be taken into account. Any power to prevent the doing of the act must be taken into account. On the other hand, in the particular circumstances of a given case, the nature of the power and the consequences of exercise of the power would be relevant considerations in determining whether, in all of the circumstances, it should be concluded that a particular act had been authorised. Similarly, the nature of any relationship between an alleged infringer and the person who does the act will have a bearing on whether, in the particular circumstances of a given case, the rights arising from the relationship and the consequences of exercising or enforcing such rights must be taken into account in determining whether it was reasonable to have exercised the power to prevent the doing of the relevant act.

180 The language of s 101(1A)(c) assumes that an alleged infringer might be in a position to take steps to prevent a relevant act, by reason of the matters referred to in s 101(1A)(a) and

s 101(1A)(b). That is to say, the language assumes that an alleged infringer might exercise a power to prevent the doing of the act concerned and might exercise or enforce rights that exist by reason of a relationship existing between the alleged infringer and the person who does the act concerned. The purpose of the enquiry called for by s 101(1A)(c) is to determine whether there are any steps, being reasonable steps, beyond exercising such a power or enforcing or exercising any rights arising from such a relationship.

Sections 101(1A)(a) and 101(1A)(b)

181 The customer relationship agreement between iiNet and each of its customers prohibited the use of the iiNet service to infringe copyright and contained a contractual right on the part of iiNet to warn its customer and subsequently terminate the service if a breach of provisions of the customer relationship agreement occurred. Breach entitled iiNet to cancel, suspend or restrict the service without notice and without recourse.

182 iiNet had a range of measures available to it, including warning customers, blocking sites or ports, and suspending or terminating the account of a customer whose account was found to have been involved in infringements of copyright. It was possible to warn a customer that an infringement, by use of the service provided to that customer, had been detected. iiNet frequently communicated warnings to its customers using a variety of means, including email. It used those means throughout the period when the Infringement Notices were being sent to iiNet.

183 iiNet had the technical capability to suspend and terminate accounts and indeed it did so from time to time on the ground of non-compliance with contractual obligations to pay fees. Termination of a customer's account would constitute a step that would prevent that customer from infringing by use of the service provided by iiNet, although such a customer could, of course, arrange for provision of service by another service provider. Nevertheless, it is clear enough that iiNet thereby had the power to prevent future acts of infringement committed by users of the service provided by iiNet to its customers.

184 iiNet did not dispute that it regularly implemented such measures, but contends that, while it routinely resorts to such measures in its business, it would have been unreasonable to use those measures to prevent acts of infringement on the part of users of the services

provided by it. However, where iiNet suspended and terminated the account of a customer, as it did on occasion, the customer, and anybody who used the service provided on the account of that customer, would have limited or no internet access. That does not appear to have been regarded as an unreasonable consequence.

185 iiNet contends that the only relevant power available to it to prevent infringement was to warn a customer, and then terminate or suspend the customer's account, and that warning alone was unlikely to be effective. iiNet says that any customer whose account is being used to infringe would already have ignored warnings contained in the customer relationship agreement and repeated on iiNet's website.

186 There was no finding by the primary judge that infringing acts engaged in by iiNet users were engaged in, in circumstances where the customer whose account was being used knew, or had reason to suspect, that infringement was involved. It may well be that an iiNet user would not know that, by downloading the Films by means of the BitTorrent System, there was infringement. It may be that an iiNet customer was unaware that the service provided to that customer was being used for infringement. A warning, coupled with reference to the entitlement of iiNet to terminate the service, may well be sufficient to persuade a customer to desist from engaging in such conduct or to take steps to ensure all users of that customer's service desist. It is one thing to be aware of a prohibition on infringement of copyright. It is another thing to be aware that specific acts engaged in actually constitute infringement.

187 It may be possible that some, or indeed many, customers would disregard a warning given by iiNet. However, it does not follow, from that possibility, that all customers would disregard a warning or even that most customers would do so. Even if many customers may disregard a warning, compliance by others would prevent further infringement involving the accounts of those customers from taking place. Every time a user of the internet leaves a BitTorrent swarm, the supply of copyright material made available online within the swarm would be reduced and the opportunity for other internet users to infringe copyright would therefore also be reduced.

188 Giving clearly worded and accurate warning to a customer whose account was thought to be involved in acts of infringement is a reasonable step that could have been taken

by iiNet, regardless of whether the warning would have been heeded by every customer. There is no basis for concluding that all, or even a substantial proportion, of iiNet's customers would permit their accounts to continue to be used for acts of infringement if they were properly warned that the acts constituted infringement and their attention was drawn to their contractual obligations and iiNet's contractual right to enforce those obligations by suspension or termination.

189 Even where a service provider such as iiNet has the benefit of the Safe Harbour Provisions, the Court is specifically empowered, under s 116AG(3)(b), to order termination of a specified account. It can hardly be concluded, therefore, that termination was, *per se*, unreasonable. Rather, the Copyright Act itself contemplates such a step. Accordingly, it must be regarded as a reasonable step, at least in some circumstances, including circumstances involving repeat infringements, to terminate or suspend an account of a customer.

190 Section 101(1A)(a) requires an enquiry as to whether iiNet had the power to prevent infringement, not whether the steps that it might take to prevent infringement might adversely impact on a customer whose account is involved in the acts of infringement. Even if the step of suspending or terminating could fairly be characterised as penal, such that relief might be granted by a court of equity, a condition of the grant of such relief would be establishing the capacity and the inclination of the customer to abide by the terms of the relevant contract. iiNet undertook the steps of warning, suspending and terminating customers' accounts for non-payment of fees. Those steps would be just as much penal in those circumstances as when taken in order to prevent infringements of copyright.

191 The fact that the service provided by iiNet may be used for purposes that do not involve acts of infringement is really of no relevance. A finding that the service provided by iiNet is also used for non-infringing purposes does not preclude a finding of authorisation of infringing acts using that service. The question of substantial non-infringing use arises only where an alleged authoriser does not have power to prevent. That is to say, the alleged authoriser does not have control over the alleged infringing acts. Where the alleged authoriser has such power to prevent, so as to have control over the use in question, it does not matter that some other use might not infringe.

192 There is a direct contractual relationship between iiNet and each of its customers. There is also a non-contractual, more distant, relationship between iiNet and iiNet users who are not actually parties to the customer relationship agreement. There is nothing in s 101(1A) that requires that there be a commercial interest on the part of the alleged authoriser in having the acts of infringement continue. iiNet provided the service by use of which infringing acts were occurring. iiNet had the contractual obligation to provide the service and its customer had the contractual obligation that the service not be used to infringe. That relationship was both contractual and technical.

193 Thus, iiNet had the capacity to control the use of its services by its customers and to take steps to prevent acts of infringement by the use of services provided to them. In some circumstances, iiNet did in fact exercise control over the provision of its services. The presence of such provisions amounted to a degree of power to prevent further acts of infringement that was significant, for the purposes of s 101(1A)(a). That power arose from the relationship between iiNet and its customers under the customer relationship agreements, the nature of which is significant for the purposes of s 101(1A)(b).

194 There is no reason to conclude that sending warnings would be unreasonable, given that iiNet's business routinely involved sending warnings to users in a variety of circumstances, such as when fees were overdue. There is no reason to view a temporary suspension as unreasonable, particularly when iiNet had the right to terminate the service altogether. The period of a temporary suspension would be a matter for consideration in any given case. A very long suspension for a very minor infringement may be unreasonable. However, that is not a reason for concluding that no suspension could ever be reasonable.

Section 101(1A)(c)

195 The language of s 101(1A)(c) requires an enquiry as to any steps that were taken by iiNet and whether there were reasonable steps that were not taken. The Infringement Notices specifically invited iiNet to cancel, suspend or restrict the accounts of the customers identified in the spreadsheets enclosed with them. Merely having a contractual provision relating to copyright infringement and drawing attention to the contractual provision on its website is hardly an effective step to prevent infringement, in circumstances where iiNet does not enforce the contractual provision.

196 iiNet says, nevertheless, that termination of an account was not a reasonable exercise of a power to prevent because it would involve disconnection of the customer from the internet. Disconnection would not, in itself, prevent infringement because of the possibility of the customer obtaining access to the internet through another carriage service provider. On the other hand, disconnection would do much more, in that the whole relationship between iiNet and its customer would be ended, thereby foreclosing all internet activity by that customer by means of iiNet's service.

197 However, it is difficult to see why that consequence is unreasonable, if the customer, having been warned that the service being provided to the customer by iiNet was being used to engage in infringing acts, that to do so was a breach of contract and that continuing to do so may result in termination, nevertheless chooses to continue to permit the iiNet service to be used to engage in infringing acts. It may be unreasonable to terminate an account without warning. However, that is not the question.

198 iiNet asserts that the Copyright Owners' difficulty in pursuing individual customers whose iiNet services are used to engage in acts of infringement is the motivation for the commencement of the proceeding against iiNet. That is to say, it is far more efficient for the Copyright Owners to pursue service providers such as iiNet than individual iiNet users. iiNet asserts that that policy consideration does not of itself justify the parting from well established principles of authorisation. That assertion, of course, begs the question. It is not to the point to say, as iiNet does, that iiNet users have infringed copyright and that such iiNet users are appropriate respondents in an infringement proceeding. Such a proposition ignores the effect of s 101(1), namely, that authorisation is a separate wrongful act over and above the primary act of infringement by an iiNet user.

199 The question is whether or not iiNet has authorised acts of infringement by its customers within s 101(1). If it has not, the proceeding should be dismissed. If it has, the Copyright Owners may be entitled to some relief. The motivation for the Copyright Owners in pursuing iiNet or other service providers is irrelevant, providing the Copyright Owners can establish authorisation of infringing acts by the service provider. On the other hand, of course, the practical difficulties that might face the Copyright Owners in pursuing individual infringers is not a justification for construing s 101(1) in any particular way, except to the

extent, if at all, that such a consideration is to be found in the amendment made by the insertion of s 101(1A).

200 The Copyright Owners contend that there is a benefit to iiNet from infringing conduct by use of its services. However, as a general rule, iiNet has more customers on its lower to middle quota plans. Only about one percent of iiNet's residential customers take the highest quota plan. Further, most customers use less than one half of their allocated quotas each month. Those facts are inconsistent with a characterisation of iiNet's business as aiming to have all customers on the largest plan possible. iiNet's primary objective is to get customers online and to give them the plan that best suits their needs. Accordingly, iiNet's objective is not just to sell as much quota as possible. As identified above, as a general rule, as usage increases, the cost to iiNet increases. A customer who uses the whole of the quota for the month pays the same fee as a customer on the same plan who uses no part or a very little part of the quota for the month. There is no basis for concluding that iiNet necessarily benefits from increased usage by reason of infringing usage. On the other hand, iiNet clearly benefits from the maintenance of the contractual relationships with its customers.

201 iiNet emphasises its Freezone service, whereby a diverse range of licensed material is made available to customers to be streamed or downloaded, where the downloading or streaming is not counted against the customer's quota. Some 44 percent of the Films are available for purchase and download from Apple iTunes by means of iiNet's Freezone service. iiNet contends that the provision of the Freezone service operates to promote the consumption of copyright material, including copyright material provided by the Copyright Owners, in a non-infringing way.

202 A large number of iiNet customers use the Freezone service. Indeed, iiNet claims to be a leader in the industry in making material available legally through its Freezone service. iiNet was the first Australian service provider to offer quota free access to online stores such as iTunes and the iView service. Because of factors such as the financial benefits to customers, fast speeds, reliable streaming and the promotion of Freezone by iiNet, the Freezone service encourages users to download and stream copyright material legitimately. iiNet contends, therefore, that the Freezone service benefits the Copyright Owners and other owners of copyright material, as well as iiNet and its customers.

203 However, the fact that iiNet provides a service whereby its customers and other users can download or stream copyright material without infringement is irrelevant to the question of whether iiNet is authorising other acts that do involve infringement of copyright. The availability of the Freezone service may be an inducement to some iiNet users, who would otherwise do acts of infringement, not to do those acts of infringement. Nevertheless, if iiNet is, at the same time, authorising other iiNet users to do acts of infringement, the Freezone service can be seen as resulting in a reduction of the scope of iiNet's infringement by authorisation but not the elimination of infringement by authorisation.

204 iiNet accepts that it had general knowledge of copyright infringement by use of the services provided to its customers. However, it contends that it had knowledge at a level of abstraction that was difficult to act on in any meaningful way. iiNet says that the only evidence of infringement at a level of specificity was the Infringement Notices but that the Infringement Notices did not make clear that the information provided by them was different from thousands of unreliable robot notices received from overseas. It says that, if a positive response was to be expected, AFACT should have explained in detail, when providing the Infringement Notices, how the allegations of infringement came to be made. iiNet says that AFACT was not entitled to keep its method of investigations secret if it expected a carriage service provider such as iiNet to be convinced of the reliability of the allegations of infringement and to act on such allegations. iiNet contends that it was not unreasonable for it to take the position that it wanted an independent third party to attest to the reliability and authenticity of the evidence provided by the Infringement Notices.

205 It was not reasonable to require iiNet to undertake the immense amount of work, cost and effort required in order to set out, review and analyse the allegations in the information provided with the Infringement Notices. iiNet did not have the guidance, which was subsequently afforded to it in the course of the proceeding, to enable it to carry out that task. I do not consider that knowledge acquired by iiNet in the course of the proceeding can be relied upon to support the case of the Copyright Owners.

206 The differences as to the legal interpretation of the information, as to the number and nature of alleged infringements highlight the sometimes difficult judgment that iiNet would be required to make in the course of implementing any kind of regime to deal with the

allegations made in the Infringement Notices. iiNet contrasts that task with the simplicity of terminating a customer's account for non payment of fees. In such a case, iiNet would not need evidence from a third party to establish that a customer has failed to pay fees.

207 iiNet receives allegations of infringement involving in excess of 5,000 IP Addresses per week. For iiNet to implement a regime of warning and suspending or terminating customers' accounts, in response to allegations of copyright infringement, an automated process would be required. It is not clear that such automation could be achieved easily. It would be necessary to create a system whereby sufficient information concerning the allegations is communicated to the relevant customer, acknowledgment of receipt by the customer was secured and cross checking for earlier notifications in respect of the same customer was undertaken. Choices would need to be made in the design of such a system, as to the number of warnings that should be given, whether there should be a period of grace, whether all alleged infringers should be treated the same or graded according to severity. Each of those choices adds complexity to the design of a system. iiNet would also need to implement and maintain additional customer support capability since the implementation of such a system would lead to queries and complaints from customers. Senior personnel would need to be involved in the handling of such queries and complaints. Even if such a system is feasible, it would be likely to involve significant expense being incurred by iiNet.

208 Mr Michael Malone, the managing director and chief executive officer of iiNet, gave evidence that, because of the high level of uncertainty as to how the possible steps outlined above might be implemented, it was not possible to estimate the cost of implementing and maintaining such a system. Mr Malone asserted that he could not justify commercially the implementation of a regime by which iiNet would threaten to deny a customer the benefit of iiNet's customer relationship agreement with that customer, in circumstances where allegations of infringement were not proved, iiNet was unable to determine the responsibility of the customer for some alleged improper conduct by an unidentified user and there was potential for significant personal and commercial disruption in the event of disconnection.

209 The Infringement Notices only gave rise to a level of particular knowledge of likely infringing activity after they had been analysed by cross checking each line of data for IP Address and time stamp, interrogating iiNet databases, identifying the account to which a

particular IP Address was assigned at a particular time and adding Peer ID data. Only after all that had been done could a step be undertaken by iiNet, in the light of any specific knowledge that could be gleaned from the Infringement Notices. iiNet says that it was not reasonable for it to be required to undertake such an analysis.

210 I consider that, before it would be reasonable for iiNet to take steps within the meaning of s 101(1A)(c) to suspend or terminate a customer's account, at least the following circumstances should exist:

- iiNet has been informed in writing of particulars of specific primary acts of infringement of copyright of the Copyright Owners, by use of particular IP Addresses of iiNet customers.

- iiNet has been requested in writing to take specific steps along the following lines in relation to such primary acts of infringement:

    (a) iiNet should inform its customer of the particulars of the allegations of primary infringement involving the use of that customer's iiNet account.

    (b) iiNet should invite the customer to indicate whether the service has been used for acts of infringement as alleged.

    (c) iiNet should request the customer either to refute the allegations or to give appropriate assurances that there will be no repetition of the acts of infringement.

    (d) iiNet should warn the customer that, if no satisfactory response is received within a reasonable time, perhaps 7 days, the iiNet service will be suspended until such time as a reasonable response is received.

(e) iiNet should warn the customer that if there are continued acts of infringement by use of the service, the service will be terminated.

(f) iiNet should terminate the service in the event of further infringements.

- iiNet has been provided with unequivocal and cogent evidence of the alleged primary acts of infringement by use of the iiNet service in question. Mere assertion by an entity such as AFACT, with whatever particulars of the assertion that may be provided, would not, of itself, constitute unequivocal and cogent evidence of the doing of acts of infringement. Information as to the way in which the material supporting the allegations was derived, that was adequate to enable iiNet to verify the accuracy of the allegations, may suffice. Verification on oath as to the precise steps that were adopted in order to obtain or discern the relevant information may suffice but may not be necessary.
- The Copyright Owners have undertaken:
  - to reimburse iiNet for the reasonable cost of verifying the particulars of the primary acts of infringement alleged and of establishing and maintaining a regime to monitor the use of the iiNet service to determine whether further acts of infringements occur, and
  - to indemnify iiNet in respect of any liability reasonably incurred by iiNet as a consequence of mistakenly suspending or terminating a service on the basis of allegations made by the Copyright Owner.

211 There are good reasons for concluding that the first and second of the circumstances set out above were substantially satisfied by the Infringement Notices in the present case. However, in relation to the third circumstance, the Infringement Notices are no more then assertions. No means of verification was furnished. More importantly, in relation to the fourth circumstance, the Copyright Owners have not offered to reimburse iiNet for any costs incurred in complying with the demands made by the Infringement Notices.

Section 112E

212 It is common ground that iiNet is a carriage service provider within the meaning of s 112E of the Copyright Act. It is also common ground that facilities that it provides to its customers are facilities within the meaning of s 112E.

213 Section 112E is located in Division 6 of Part IV of the Copyright Act, in which s 101 is found. Accordingly, when s 112E speaks in terms of a person who **authorises** an infringement, it is necessary to have regard to the provisions of s 101 and the jurisprudence relating to its interpretation, in order to give meaning to that term. A statute is not to be construed in a fashion that results in some sentence, clause or word being superfluous, void or insignificant if another construction is available under which the sentence, clause or word is made useful and pertinent (see *Project Blue Sky Inc v Australian Broadcasting Authority* (1998) 194 CLR 355 at 382). Thus, s 112E must have some work to do. That is to say, there must be circumstances where a person will be found to have authorised an act within the meaning of s 101 but will be excused from the consequences of having done so by the operation of s 112E. The non-exhaustive collection of matters referred to in s 101(1A) indicates that a person does not authorise an act of infringement merely by providing facilities that are used to do an act of infringement, and nothing more.

214 iiNet contends that, in the light of the objects of the Digital Agenda Act, which are described above, s 112E should be construed beneficially, so as to give all of the relief to a provider of facilities that a fair reading of the language of s 112E will allow. It would be antithetical, iiNet says, to the certainty sought to be achieved, and the objectives of the reforms of the Digital Agenda Act, to exclude from s 112E circumstances where factual elements relevant to authorisation arise beyond the provision of facilities. iiNet says that the section requires something more than mere knowledge of infringement. It says that considerations of certainty and efficient operation of information technology industries will be jeopardised if all that is needed to defeat s 112E is to assert to a carriage service provider that infringements are occurring by use of the carriage service provider's facilities.

215 iiNet contends that s 112E will apply unless the relevant conduct of a carriage service provider goes beyond **that which is within the ordinary scope of the provisions of the facilities in question**. It says that merely acquiring knowledge, much less suspicion, of acts

on the part of others, as a consequence of or as an incident of the provision of the facilities, would not suffice.

216 However, s 112E makes no reference to conduct of an alleged authoriser that is within the ordinary scope of the provision of the facilities. Rather, the reference is to the **mere** use of the facilities by an infringer. That is the circumstance to be excluded from the ambit of authorisation. The construction contended for by iiNet places a gloss on the words of s 112E and fails to give the word **merely** any operation, despite its central part in the effect of the provision.

217 A critical aspect of the language of s 112E is the use of the word **merely**. That is to say, a carriage service provider will not be taken to have authorised an infringement of copyright by reason only of the fact that facilities provided by the carriage service provider were used for the infringement. There is work for s 112E to do where a service carriage provider has no knowledge of an infringement. Section 112E presupposes that a person who merely provides facilities for making a communication might, absent s 112E, be taken to have authorised an infringement of copyright effected by use of the facility (see *Cooper* at [32]). A finding of authorisation may be made in cases involving a general permission or invitation implied by the provision of facilities, without the need for the presence of other factors, such as knowledge of particular acts of infringement (see *Moorhouse* at 21).

218 The nature and context of s 112E do not support the proposition that it should necessarily be construed in favour of the provider of facilities. The provision operates alongside a series of provisions, including s 101(1A), the object of which is to provide the owners of copyright with a right of action to prevent unauthorised use of copyright material. There is nothing in the language of s 112E to suggest that it provides a general immunity for carriage service providers to conduct their businesses regardless of the circumstances.

219 Section 39A was introduced in 1980 in response to the decision in *Moorhouse*. Section 39A provides, in effect, that the operator of a library is not to be taken to have authorised the making of an infringing copy on a machine at the premises of the library, such as a photocopier, **by reason only** that the copy was made on that machine. The precondition for relying on that exemption is that a prescribed form of notice is displayed on or near the

machine. Thus, s 39A addresses the circumstances where copies are made on a machine supplied by the library.

220 Section 39A clearly and directly provided certainty for libraries, by providing that the installation of a warning notice in the prescribed form would avoid liability. On the other hand, provision of facilities *simpliciter* does not establish authorisation and s 112E does not provide any equivalent certainty or guidance in the way that s 39A does. Thus, iiNet says, if the Copyright Owners' construction of s 112E were accepted, a contractual relationship between the provider of the facilities and its customers, some of whom may infringe copyright, would remove the provider of the facilities from the ambit of s 112E because the relationship is a factor under s 101(1A) relevant to authorisation.

221 Section 39B is similar in its operation to s 112E. Section 39B corresponds precisely with s 112E in relation to infringement of copyright in a **work**, rather than a copyright in an audiovisual item, such as a film, as provided in s 112E. Both s 39B and s 112E address the circumstance of the use of facilities for the doing of infringing acts. But for the presence of those provisions, the provider of the copier in a library or the provider of communication facilities might be held to have authorised infringement.

222 To the extent that it is relevant, the extrinsic material makes clear that the word **merely** was intended to have some real operation. The legislative purpose is evident in the light of the treaty obligations that s 112E was intended to implement. The obligations are contained in an agreed statement made by the 1996 Diplomatic Conference adopting Article 8 of the WIPO Copyright Treaty to the effect that it is to be understood that the **mere provision of physical facilities** for enabling or making a communication does not **in itself** amount to communication within the meaning of the treaty or the Berne Convention. Section 112E was directed to the implementation of that obligation. Hence, the relevant part of the explanatory memorandum for the Bill for the Digital Agenda Act gave the example of a service provider not being liable for having authorised a copyright infringement **merely by providing the facilities** by which the communication was facilitated.

223 To suggest that s 112E is concerned only with that which goes beyond what is in the ordinary scope of the provision of the facilities in question would give rise to uncertainty and would vary according to the ambit of a carriage service provider's current activities. There is

nothing in the objects of the Digital Agenda Act to suggest that the provisions of s 112E were necessarily intended to benefit service carriage providers. Further, an additional object of the Digital Agenda Act is to ensure the efficient operation of relevant industries in the online environment by providing a practical enforcement regime for copyright owners.

224 The Copyright Owners contend that iiNet had sufficient knowledge of relevant acts of infringement to enable it to act, but took no action to prevent or avoid future acts of infringement. Further, iiNet's contractual relationship with its customers enabled it to take steps. iiNet accepts that its contractual rights would entitle it to suspend or terminate the provision of services to customers on the grounds of infringement. Nevertheless, it chose not to exercise those rights. iiNet justified the continued supply of services to customers where the service is used for acts of infringement on the basis that to take any action to impose restrictions on the use of the service, such as the suspension of access, would cause iiNet commercial harm in that the customer may cease to use the services of iiNet and take services from a competitor.

225 The Copyright Owners contend that in any event, iiNet's conduct went beyond that which is within the ordinary scope of the provision of the facilities in question. They point to iiNet's knowledge of the infringements, coupled with the fact that iiNet took no action to prevent or avoid future acts of infringement. That, they say, amounts to conduct outside the ordinary scope of the provision of the facilities in question. The relevant knowledge came, for the most part, from the Infringement Notices. The ordinary provision of communication facilities by a carriage service provider does not involve providing or continuing to provide access to persons who are known to be using the service for infringing copyright, in breach of the terms and conditions upon which the carriage service provider provides the service, including a term that purports to prohibit such activity.

226 iiNet contends that it was central to the argument in *Moorhouse* that the invitation implied by the provision of the photocopier extended to the doing of acts comprised in the copyright of authors whose books were on the library shelves. Authorisation was given to use the photocopier to copy library books. The operator of the library provided the copyright material in addition to providing the photocopying machine that was the means of infringement. iiNet contends that the statutory scheme, requiring consideration of the matters

referred to in s 101(1A), would be irrelevant if authorisation could arise merely from the provision of facilities without knowledge.

227 Further, iiNet says, if the construction contended for by the Copyright Owners were accepted, a carriage service provider would be denied the protection of s 112E once it had acquired knowledge of infringements arising from use of its facilities. A provision so construed would not provide clarity or guidance, iiNet says, if, at any moment, a provider might be denied its protection merely because someone makes allegations of infringement. iiNet says that the position of the Copyright Owners is that a provider who would otherwise be entitled to the protection of s 112E is deprived of that protection and rendered an infringer simply because someone such as AFACT makes written allegations of copyright infringement arising from the use of the facilities.

228 That argument, of course, raises the question of whether a carriage service provider is bound by mere assertion or whether it is entitled to require corroboration or evidence. The mere assertion or allegation of acts of infringement may not suffice to constitute knowledge. However, if the circumstances outlined above in dealing with authorisation within s 101(1) are shown to exist, the position will be different. Where those circumstances exist, s 112E will not afford an answer. That is to say, in those circumstances, iiNet would not then be **merely** providing facilities.

Part 13 of the Telco Act

229 The Copyright Owners assert that there were various steps that iiNet could and should have taken, once it had been provided with the allegations made in, and the information provided with, the Infringement Notices. iiNet contends that it was not lawful or reasonable for iiNet to take those steps because of the prohibition in Part 13 of the Telco Act. Thus, iiNet points to s 276, which makes it a criminal offence for certain use or disclosure of protected information by a carriage service provider or its employees. iiNet contends that none of the exceptions in ss 279, 280, 289 and 290 applied in the circumstances and that, as a consequence, s 276 of the Telco Act applied to the use or disclosure of the information. Therefore, iiNet contends, it did not have the power to prevent the infringement of copyright by one of its customers, within the meaning of s 101(1A)(a) of the Copyright Act, and it would not have been reasonable, within the meaning of s 101(1A)(c) of the Copyright Act,

for iiNet to take any steps inconsistent with that prohibition, when such steps would have constituted a criminal offence.

230 iiNet would need to use three different kinds of information in order to warn a customer or to suspend or terminate provision of services to a customer. The three kinds of information are as follows:

- The IP Addresses and times and other information provided by the Infringement Notices (**AFACT information**).
- Information identifying the IP addresses that were allocated to particular iiNet customers at particular times (**Score information**).
- Information as to the personal details, such as names, addresses, email addresses and telephone numbers, of iiNet's customers (**Rumba information**).

231 The AFACT information included, in addition to IP addresses and times, information about the hash value of each downloaded file, the identity of the Film involved and the size and extent of the downloaded file and other data. The Score database records the assignment of iiNet IP addresses to particular iiNet accounts. It has an interface that can find, upon insertion of an IP address, date and time, the name of the iiNet customer to which that address was allocated at that time. The Rumba database contains subscription plan details, payment details and history and other personal particulars of iiNet customers as well as the contact details of iiNet customers.

232 iiNet would have to match the AFACT information with the Score information. That would provide it with details of the customer account that was implicated in an alleged act of infringement. Once it had that Score information, it would then need to consult the Rumba information, which would contain the contact details of the iiNet customer in respect of that account.

233 It is common ground that all of the AFACT information, the Score information and the Rumba information is information within s 276(1)(a) of the Telco Act. Accordingly, the disclosure or use of that information is prohibited by s 276(1) unless the disclosure or use falls within one of the exceptions in Division 3 of Part 13. However there is a question as to

whether the AFACT information falls within s 276(1)(b)(i). If it does not, s 276(1) would not apply to it.

234 The effect of s 276(1)(b) is that the prohibition in s 276(1) only applies to the disclosure or use of information by a carrier or carriage service provider if the information comes to the knowledge of the carrier or provider, or into its possession, **in connection with** its business as such a carrier or provider. iiNet says that the essence of the Infringement Notices is the repeated assertion that iiNet, as it carries on its business, wrongly permitted users of iiNet services to make Films available online using the BitTorrent System. The Infringement Notices invite iiNet to take some sort of action, and that that action entails adapting or changing the way it carries on its business of providing the service of connecting its customers to the internet. iiNet says that the AFACT information, therefore, was very clearly provided to iiNet in connection with its business as a carriage provider. Accordingly, it says, the AFACT information satisfies the statutory requirement in s 276(1)(b).

235 However, information gathered on the internet by a third party, such as AFACT or DtecNet, and supplied to a carriage service provider without restriction, does not satisfy the requirement that it comes to iiNet's possession or knowledge in connection with its business. The words **in connection with** must be construed with regard to the context and purpose of the provision in which they appear. Section 276 is directed to protecting information of the type that is acquired by an employee of a carriage service provider by virtue of the carriage service provider's being in a position peculiarly to acquire information of that type. Information that did not start out as confidential does not change its character and become subject to the restrictions of s 276 merely because it leaves AFACT and comes into the possession of iiNet. The effect of iiNet's construction would be to preclude it from using any public information concerning its customers, even if such information were published in a daily newspaper. Section 276(1) is not satisfied in relation to the AFACT information.

Section 279

236 Under s 279(1), s276 does not prohibit a disclosure or use **by a person** of information if, relevantly, **the person** is an employee of a carriage service provider and the disclosure or use is made in the performance of the person's duties as such an employee. iiNet contends that the exception in s 279(1) operates only in respect of an employee of a carriage service

provider and not in respect of the carriage service provider itself. Thus, it says, if iiNet had used the AFACT information, the Score information or the Rumba information, its employees would have been involved in that use. While the employees would be exempted from criminal liability to the extent that they used the information in the performance of their duties as employees, iiNet itself would not be exempted.

237 Having regard to the provisions of the customer relationship agreement between iiNet and its customers, and the obligation placed on customers not to commit copyright infringements, the disclosure of the relevant information to enforce the terms and conditions of the customer relationship agreement and to prevent such infringement would be conduct by an employee in the performance of that employee's duties as an employee of iiNet. The investigation of customers for possible copyright infringing activity in contravention of the terms of the customer relationship agreement would be incidental to the carrying out of the duties of an employee, being the functions and proper actions that are authorised by the employment (*Canadian Pacific Tobacco Company Limited v Stapleton* (1952) 86 CLR 1 at 6). Accordingly, acting on the Infringement Notices would constitute the performance of their ordinary duties by iiNet's employees.

238 The wording of s 279 is not limited to the protection of an employee. It exempts from s 276 **a disclosure or use** by an employee. A disclosure by an employee in the performance of his or her duties would also be a disclosure by the employer. The act of the employee is the act of the employer. Section 279 exempts the act of use or disclosure. The exception would have no practical utility if it only operated to exempt an employee from criminal responsibility when performing his or her duties but left the employer criminally responsible.

239 It is significant that s 279 constitutes the first exception in Part 13 and might therefore be expected to have the most general application. It is the only exception that purports to apply generally to disclosure or use made in the typical day to day activities that need to be undertaken by a carriage service provider. There is no corresponding exception permitting a carriage service provider itself to use or disclose information in the course of its ordinary day to day activities as a carriage service provider. That is a reason for construing s 279 as exempting **the use or disclosure** of information from the operation of s 276, rather than exempting only an individual person from using or disclosing information.

240 That construction is supported by the language of the other exceptions in Division 3 of Part 13. Other exceptions apply in more limited circumstances and depend on such matters as consent. Section 291 is relevant in that context. Section 291 provides that s 276 does not prohibit disclosure or use by a person if it is for the purpose of, or is connected with the business of, any **other** carrier or carriage service provider. Thus, there is an exception for use or disclosure of information by one carriage service provider if it is necessary for the conduct of the business of **another** carriage service provider. There is no corresponding exception dealing expressly with the first carriage service provider, other than s 279, construed as indicated above. It would be anomalous if there were an exception for one service provider to disclose information to another service provider, or use it for that purpose, but no exception for the carriage service provider to use or disclose the information in connection with its own activities.

241 In addition, the other exceptions in Division 3 apply generally, without drawing a distinction between the exemption for an employee on the one hand, and not for an employer on the other. Where there is an express exemption for an employee in the course of carrying out the employee's duties, the exemption should be construed as affording the same exception to the employer in respect of those duties.

Section 280

242 The effect of s 280(1)(b) is that s 276 does not prohibit a disclosure or use of information if the disclosure or use is required or authorised by or under law. The Copyright Owners say that the effect of s 101(1A) of the Copyright Act and the Safe Harbour Provisions is to require or authorise use or disclosure. A condition of the statutory limitation contained in the Safe Harbour Provisions is that a service provider must adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers. That is the effect of item 1 in the schedule to s 116AH(1). The Copyright Owners say that the effect is **to oblige** a carriage service provider to take steps to satisfy the relevant condition if it is to obtain the benefit of the relevant limitation on remedies. Therefore, they say, a carriage service provider is authorised to take such steps as are appropriate for that purpose. Further, they say, one of the factors to be taken into account under s 101(1A) is whether the alleged authoriser has taken reasonable steps to prevent or avoid an act of infringement, including pursuant to any industry code of practice. Therefore,

they say, a person would be authorised to take such steps in order to avoid infringement. Otherwise, they say, a service provider could not take steps to comply with an industry code if that involved the use or disclosure of information within s 276(1).

243 However, s 101(1A) does not expressly or impliedly require or authorise the disclosure or use of a document or information of the character described in s 276(1). The Safe Harbour Provisions simply provide that, if certain prerequisites are satisfied by a carriage service provider, certain consequences may follow in terms of relief in infringement proceedings. Those provisions do not require disclosure within the meaning of s 280. On the other hand, they may be thought to authorise disclosure. A carriage service provider must satisfy certain prerequisites before it can take advantage of the limitations on relief afforded by the provisions. A carriage service provider must be taken to be authorised to take reasonable steps to satisfy those prerequisites.

Section 289

244 Section 289 relevantly exempts disclosure or use by a person of information or a document if the information or document relates to the affairs or personal particulars of another person and that other person:

- 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
- has consented to the disclosure or use, as the case requires, in the circumstances concerned.

245 The Copyright Owners contend that the second exception is applicable, because the effect of the relevant provisions of iiNet's customer relationship agreement is to secure the customer's consent to the use of relevant information for various purposes, including administering and managing the services provided by iiNet and the customer relationship agreement. They say that, since the terms of the customer relationship agreement prohibit the use of the services for copyright infringing purposes, the investigation of such an activity forms part of such permitted purposes.

246 The Copyright Owners say that, having regard to the totality of the relevant provisions of iiNet's customer relationship agreement, each customer was required to ensure that the service was not used to infringe the copyright of others. Express authorisation was therefore given to iiNet to monitor communications for the purpose of ensuring compliance with the customer's obligations and to collect information reasonably capable of identifying a user for the purpose of administering and managing the service and the customer's account. They say that express authority was given for the use of a customer's confidential information to the extent necessary to exercise iiNet's rights under the customer relationship agreement. Cancellation or suspension for breach could only be effected by notice to the customer of such cancellation or suspension, with the option of giving prior notice. The parties must have contemplated that such notice would include identification of the nature of the breach.

247 The Copyright Owners point to clauses 4.1, 4.2, 4.4, 12.3, 14.2, 14.4 and 21.1 of the customer relationship agreement. Clause 20.1(a) provides that iiNet can use or disclose confidential information of the customer to the extent necessary to perform obligations or exercise rights under the customer relationship agreement. Clause 4.4 authorises iiNet to monitor usage of the service and the communications sent over it for the purpose of compliance with the customer relationship agreement. The fact that the monitoring is not done by iiNet does not preclude that from being information that iiNet was authorised by its customers to use for the purpose of monitoring the usage of the customer's account.

248 Section 289 applies only to one of three relevant classes that protect information and documents referred to in s 276. The language of s 289 indicates that the provision is directed to the category referred to in s 276(1)(a)(iv), namely, the affairs or personal particulars of another person, including telephone numbers and addresses. The language of s 276(1)(a)(iv) should not be given a construction that renders the categories in (i), (ii) and (iii) superfluous. While there may be some instances of overlap, the statutory enumeration of different categories in s 276 requires recognition and application in construing s 289. iiNet contends that the AFACT information included information about the contents or substance of the communication carried by iiNet and the carriage services supplied by iiNet, which are not within s 289.

249 Clause 12.3 of the customer relationship agreement relevantly provides that iiNet may collect, use and disclose **Personal Information** about the customer for the purposes of:

- providing the services required by the customer from iiNet and iiNet related entities, and
- administering and managing those services, including billing, account management and debt collection.

Personal Information is defined as information or opinion about the customer from which the customer's identity is apparent or can reasonably be ascertained, and includes name, current and previous addresses, service number, date of birth, email address, bank account or credit card details, occupation, drivers licence number and credit card information and credit rating.

250 Clause 12.3 refers only to Personal Information, being information that either reveals the identity of the customer or from which the identity of the customer can reasonably be ascertained. AFACT information includes information that falls outside the scope of Personal Information. For example it includes the identity of the Film and some information about the extent to which it was made available and downloaded, each of which reveals the substance or content of the communication carried by iiNet. AFACT information also includes the fact that carriage services have been supplied to a person at a particular time or times. The use by iiNet of that information would be outside the agreement in clause 12.3 because it is outside the meaning of Personal Information.

251 iiNet also contends that clause 12.3(d) does not amount to consent for the purpose of s 289, because AFACT information may record information about the activities of a third person who uses the iiNet's customer's account, who is not a party to the customer relationship agreement. iiNet also says that the terms of the purpose identified in clause 12.3 are insufficiently specific to permit a conclusion that the customer has consented to use of information in the circumstances with which the present case is concerned. iiNet says that the customer relationship agreement reflects an agreement, at a high level of generality, that the customer will not use the services provided by iiNet illegally or in a way that infringes the rights of another person. It also provides, at an equally high level of generality, that iiNet may restrict, suspend or cancel the service if the customer breaches a material term or misuses the service or if iiNet reasonably suspects fraud or other illegal conduct by the customer or another person. iiNet says that, in that context, agreement to the use of Personal

Information for the purpose of administering and managing a customer's internet service could not reasonably be taken to amount to consent to use of that information in order to suspend or terminate the customer's account in response to the representations of an agent of a third party whose copyright a user of the customer's account has allegedly infringed. Those steps are different from the general administration and management of a customer's internet account. For those reasons, I would be disposed to conclude that s 289 does not provide an exception that would have applied to the conduct of iiNet, had it taken, in response to the Infringement Notices, the steps advocated by the Copyright Owners.

Section 290

252 The effect of s 290 is that s 276 does not prohibit a disclosure or use by a person of information if the information or document relates to the contents or substance of a communication made by another person and 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.

253 The words of s 290 replicate the words of s 276(1)(a)(i). The exception only operates in respect of information that relates to the contents or substance of a communication. Section 290 does not extend to the disclosure or use of information of the sort referred to in s 276(1)(a)(iii) or s 276(1)(a)(iv). Therefore, iiNet says, the exception in s 290 cannot operate to except the use or disclosure of all of the AFACT information, Score information and Rumba information.

254 Section 290 only operates where, 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, had they been aware of it. The relevant circumstances include that each user of the iiNet service is alleged to have made available copies of Films and thereby infringed the copyright of the Copyright Owners. iiNet contends that it is impossible to imagine, let alone reasonable to expect, that persons who are prepared to misuse its services for making available infringing copies of Films would have consented to the use by iiNet of information it has or is provided with about the contents or substance of their communications. I would be disposed to accept that contention.

Conclusion as to Authorisation

255 The exceptions provided for in ss 279 and 280 would be sufficient to exclude the prohibition in s 276. Accordingly, the provisions of Part 13 of the Telco Act do not stand in the way of iiNet using AFACT information, Score information or Rumba information in taking steps to prevent further infringements.

256 Further, if the circumstances outlined above in dealing with authorisation within 101(1) were shown to exist, the would be case outside s 112E. That is to say, the involvement of iiNet in the acts of primary infringement would then go beyond iiNet **merely** providing facilities to iiNet users.

257 However, while the evidence supports a conclusion that iiNet demonstrated a dismissive and, indeed, contumelious, attitude to the complaints of infringement by the use of its services, its conduct did not amount to authorisation of the primary acts of infringement on the part of iiNet users. Before the failure by iiNet to suspend or terminate its customers' accounts would constitute authorisation of future acts of infringement, the Copyright Owners would be required to show that at least the following circumstances exist:

- iiNet has been provided with unequivocal and cogent evidence of the alleged primary acts of infringement by use of the iiNet service in question. Mere assertion by an entity such as AFACT, with whatever particulars of the assertion may be provided, would not, of itself, constitute unequivocal and cogent evidence of the doing of acts of infringement. Information as to the way in which the material supporting the allegations was derived, that was adequate to enable iiNet to verify the accuracy of the allegations, may suffice. Verification on oath as to the precise steps that were adopted in order to obtain or discern the relevant information may suffice but may not be necessary.
- The Copyright Owners have undertaken:
    - to reimburse iiNet for the reasonable cost of verifying the particulars of the primary acts of infringement alleged and of establishing and maintaining a regime to monitor the use of the iiNet service to determine whether further acts of infringements occur, and

- to indemnify iiNet in respect of any liability reasonably incurred by iiNet as a consequence of mistakenly suspending or terminating a service on the basis of allegations made by the Copyright Owner.

They do not exist in the present case.

APPLICATION OF SAFE HARBOUR PROVISIONS

258 To attract the benefit of the Safe Harbour Provisions, it is necessary for iiNet to demonstrate that it has satisfied, relevantly, the condition in item 1 of the table in s 116AH(1), namely, that it has adopted and reasonably implemented **a policy** that provides for termination, in appropriate circumstances, of the accounts of repeat infringers. iiNet contends that that condition was satisfied. The Copyright Owners say that iiNet has not adopted or implemented a policy that satisfies the condition.

259 iiNet contends that its policy was to terminate the accounts of repeat infringers in three circumstances as follows:

- when iiNet was ordered to do so by a court;
- when an iiNet customer admitted to infringing copyright; or
- when an iiNet user was found by a court or other authority to have infringed.

It claims that its policy was evidenced by:

- The Internet Industry Association ICH and Safe Harbour guide;
- The iiNet copyright notice on its website; and
- iiNet's customer relationship agreement.

Mr Malone said that iiNet's policy would be triggered where there was a court order, other legislative instrument or code, a finding of repeat infringement of copyright by a court in an action where iiNet was not a party or an admission by an account holder that the account holder had repeatedly infringed copyright. iiNet asserted that none of those situations had occurred and that, therefore, the policy had not been engaged.

260 iiNet relies upon the following matters as support for its contention that it satisfied the relevant condition:

- Representatives of iiNet attended at presentations by the IIA in respect of the requirement for the application of the Safe Harbour Provision.

- Representatives of iiNet reviewed a compliance check list provided to iiNet by the IIA.

- iiNet obtained advice from the IIA regarding the treatment of non-compliant notifications of infringements received from the United States.

- iiNet developed a document entitled "IIAICH and Safe Harbour Guide", which was approved by iiNet's Chief Executive Officer and Managing Director.

- iiNet published a notice on its website setting out the contact details of the designated representative appointed pursuant to the Copyright Regulations.

- iiNet published a notice on its website to the effect that the hosting of illegal or copyright material using an iiNet service constituted a contractual breach of its customer relationship agreement and that such a breach may result in the suspension or termination of service without notice.

- iiNet instructed an external law firm to conduct a substantive review and redrafting of the customer relationship agreement, which included amendments to the sections regarding use of iiNet's services, termination and suspension provisions.

- Implementation of the Safe Harbour compliance measures were discussed at internal meetings at iiNet.

- Employees of iiNet continued to review support related emails and correspondence in relation to copyright infringement issues.

261 iiNet receives thousands of unreliable robot notices per week alleging infringement and, in the case of the Infringement Notices, thousands of entries are contained in an

unverified spreadsheet. iiNet says that it should not be required, in order to satisfy condition 1, to have a policy whereby it would be required, upon receipt of each robot notice or each of the Infringement Notices, to review, analyse and conduct secondary investigations of infringement allegations in order to ascertain whether the customer, or some other person using the customer's account, may or may not have infringed.

262 Thus, iiNet relies on the customer relationship agreement and the section of its website dealing with copyright. However, the customer relationship agreement provides no guidance as to the way iiNet will respond to copyright infringement. The copyright section of iiNet's website also provides no such guidance.

263 The explanatory memorandum published in connection with the US Free Trade Bill 2004 gives some guidance as to the purpose of the Safe Harbour Provisions. Thus, the Safe Harbour Provisions were intended to provide:

- legal incentives for service providers to cooperate with copyright owners in deterring the unauthorised storage and transmission of copyright materials; and

- limitations in the law regarding the scope and remedies available against service providers for copyright infringements that they do not control, initiate or direct and that take place through systems or networks controlled or operated by them or on their behalf.

264 The first element of iiNet's so-called policy is no more than a policy to obey the law. All three elements set thresholds that would excuse a service provider from acting on knowledge of copyright infringement, thus turning a blind eye to infringement that could be prevented. iiNet's so-called policy was not one for taking action in response to repeat infringement, and cannot constitute cooperation with Copyright Owners as required by the Safe Harbour Provisions. iiNet did not establish any processes to facilitate the operation of the so-called policy, in that it did not inform its customers of the existence of the policy. Indeed, iiNet claims it could not use information derived from the Infringement Notices, because of the operation of Part 13 of the Telco Act. Further, iiNet did not have an

operational email address to receive notices from copyright owners as required by the Regulations. That is indicative of a failure to implement a policy.

265 Condition 1 of item 1 has at least two elements, being the **implementation** of a **policy** that provides for termination of accounts. That requires the identification of a relevant policy and its implementation. It may be that iiNet had a policy as formulated by Mr Malone. It probably implemented that policy. The question, however, is whether that was a policy that provides for termination, in appropriate circumstances, of the account of a repeat infringer. The key concept in that phrase is "in appropriate circumstances". The circumstances of Mr Malone's so called policy are not appropriate circumstances so as to satisfy the condition.

266 There is a further question as to whether, on its proper construction, condition 1 of item 1 contemplates termination of an account where a person other than the account holder is a repeat infringer by means of the use of that account. iiNet contends that a repeat infringer is an account holder who himself or herself has repeatedly infringed. It says that the repeat infringer can only be the account holder because the provision refers to the accounts **of** repeat infringers. It says that, although a term of the customer relationship agreement provides that the account holder agrees not to allow anybody else to use the service for one of the prohibited uses, that cannot convert an account holder into an infringer or repeat infringer. It says that the policy must involve the step that the account holder himself or herself has in fact himself or herself infringed. Thus, it says, in order to trigger the policy, repeat infringing acts by a particular person, mainly, the account holder must be identified. Where such identification does not occur, the policy is not triggered.

267 However, the phrase, when read in context, refers simply to accounts **on** which persons have repeatedly infringed and that is consistent with the use of the word **of** to denote the relevant accounts. That construction is supported by the explanatory memorandum, which says that a service provider must adopt and reasonably implement a policy of terminating, in appropriate circumstances, t**he accounts of users who are repeat copyright infringers**. If the Parliament had intended to limit the scope of the condition to repeat infringers who were also account holders, and not apply to accounts that were used repeatedly to infringe, it would have used more precise language. That construction is also consistent with s 116AG(3)(b), which specifies the relief to be available where a service

provider complies with condition 1 of item 1. That provision refers to an order "requiring the carriage service provider to terminate a specified account" and not solely accounts used repeatedly to infringe by the holders of the accounts.

268 iiNet says that its so called policy is consistent with its construction of condition C. Under its policy, a court finding of repeated infringement will necessarily lead to the identification of an individual responsible for that infringement. Similarly, it says, an admission by an account holder will identify an individual. Either way, once in possession of that information, iiNet would be able to act in accordance with its policy and, if the policy were engaged, terminate the relevant account.

269 iiNet points out that s 116AG(3)(b) makes it clear that any order by a court is discretionary and would be subject to a number of factors that must be considered by the court, as well as any other factors the court considers relevant. Such factors might ordinarily include issues as to whether the infringements occurred as a result of the actions of an unrelated third party without knowledge or consent of an account holder or other analogous circumstances. In such cases, the court would have the discretion not to grant such a remedy.

270 iiNet also says that, on the construction contended for by the Copyright Owners, it would be necessary for iiNet to terminate all accounts where an Infringement Notice purported to indicate any repeat infringement. It says that such a construction would give s 116AG(3)(b) no work to do, since there would be no accounts remaining for the Court to order to be terminated. The contention that an account holder would be authorising an infringement and therefore be an infringer is rejected by iiNet on the basis that that would require a construction that involves the complexity and questions raised in this proceeding as to the meaning of authorisation within the meaning of s 101.

271 iiNet's construction could lead to perverse results. Thus, a policy would not be required to deal with infringing users who are not account holders. In circumstances where internet accounts are routinely used by several members of a household and where an account holder conceivably may not be the principal user of the account, such a construction would mean that only a fraction of the accounts in which repeat infringements actually occur would be required to be dealt with in a policy in order to satisfy condition 1. The construction contended for by iiNet would make it impractical for iiNet to implement such a policy,

thereby undermining its ability to rely on the Safe Harbour Provisions. Condition 1 is imposed on iiNet in order to gain the protection of the Safe Harbour Provisions. On its own construction, iiNet would need to attempt to identify, in relation to any account in which infringements were committed, whether the account holder was the actual infringer. A failure to do so would constitute the absence or non-implementation of the required policy. In any event, the customer who is the account holder would be an infringer in so far as that customer implicitly authorised the activity of the user of the account that constituted infringement.

272 The documents relied on by iiNet make no reference to repeat infringers or what iiNet may do in relation to such infringements. Customers were never made aware of the so-called policy and would be likely to argue that it formed no part of a contract for services and was therefore unenforceable. Merely attending meetings with the IIA and with other service providers, having its customer relationship agreement reviewed by lawyers and considering the issue internally does not amount to the implementation of a policy. iiNet had no processes in place that resemble a policy. There is no evidence that iiNet decided not to act on the Infringement Notices because they were not sworn or verified. For completely different reasons, iiNet decided not to act on the infringement notices, regardless of information they contained. Accordingly, if it were established that iiNet had authorised primary acts of infringement, iiNet would not be entitled to the benefit of the Safe Harbour Provisions in relation to those acts.

CONCLUSION

273 The appeal should be dismissed. The parties should be invited to make submissions as to the costs both at first instance and of the appeal.

274 Even though the Copyright Owners are not entitled to the relief claimed in this proceeding, it does not follow that that is an end of the matter. It is clear that the questions raised in the proceeding are ongoing. It does not necessarily follow that there would never be authorisation within the meaning of s 101 of the Copyright Act by a carriage service provider, where a user of the services provided by the carriage service provider engages in acts of infringement such as those about which complaint is made in this proceeding. It does not necessarily follow from the failure of the present proceeding that circumstances could not

exist whereby iiNet might in the future be held to have authorised primary acts of infringement on the part of users of the services provided to its customers under its customer service agreements.

I certify that the preceding two hundred and seventy-four (274) numbered paragraphs are a true copy of the Reasons for Judgment herein of the Honourable Justice Emmett.

Associate:

Dated: 24 February 2011

IN THE FEDERAL COURT OF AUSTRALIA
NEW SOUTH WALES DISTRICT REGISTRY
GENERAL DIVISION **NSD 179 of 2010**

ON APPEAL FROM THE FEDERAL COURT OF AUSTRALIA

BETWEEN:	**ROADSHOW FILMS PTY LIMITED (ACN 100 746 870)** **First Appellant**
	THE PARTIES IN THE ATTACHED SCHEDULE 1 **Second Appellant to Thirty-Fourth Appellant**
AND:	**IINET LIMITED (ACN 068 628 937)** **Respondent**
JUDGES:	**EMMETT, JAGOT AND NICHOLAS JJ**
DATE:	**24 FEBRUARY 2011**
PLACE:	**SYDNEY**

REASONS FOR JUDGMENT

JAGOT J

275 This appeal concerns the respondent's alleged authorisation of breaches of the appellants' copyright. The respondent, iiNet Limited (**iiNet**), is an internet service provider. The appellants are film studios owning copyright in film and television productions.

276 These reasons are divided into the following sections:

A. BACKGROUND TO THE PROCEEDING

277 The background to this proceeding is that internet service providers and copyright owners have not agreed to an industry code in respect of copyright material as contemplated by the legislature in its enactment of Div 2AA of Pt V of the *Copyright Act 1968* (Cth) (known as the "safe harbour" provisions).

278 The safe harbour provisions enable internet service providers to limit remedies against them for infringement of copyright. This protection to internet service providers is available only if conditions 1 and 2 of item 1 of s 116AH(1) of the Copyright Act are satisfied:

> 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.
>
> 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.

279 An "industry code", for the purpose of these conditions, is a code meeting the following description (reg 20B of the *Copyright Regulations 1969* (Cth)):

> (a) the industry code must be developed through an open voluntary process by a broad consensus of copyright owners and carriage service providers;
> (b) the industry code must include a provision to the effect that *standard technical measures* are technical measures that:
> (i) are used to protect and identify copyright material; and
> (ii) are accepted under the industry code or developed in accordance with a process set out in the industry code; and
> (iii) are available on non-discriminatory terms; and
> (iv) do not impose substantial costs on carriage service providers or substantial burdens on their systems or networks.

280 Any industry code so adopted would also apply for the purpose of s 101(1A)(c) of the Copyright Act (specifying matters relevant to the determination of the authorisation of copyright infringement, including compliance with any industry codes of practice).

281 After the commencement of the safe harbour provisions a voluntary process of discussions for the purpose of reaching consensus on an industry code was commenced. By December 2005 the Chief Executive of the Internet Industry Association (**the IIA**) had forwarded to the Association's members (including iiNet) a draft industry code. The draft industry code included a draft repeat infringer policy as referred to in condition 1 of item 1 of s 116AH(1), which each member was required to adopt in order to comply with the code. The proposed repeat infringer policy (contained in a schedule to the draft industry code) contained provisions in which:

- account holders (also referred to in the industry as customers or subscribers) were held responsible for copyright infringement if a third party asserted infringement or there was "good evidence" of infringement;
- "good evidence" included not only a court ruling but also a statutory declaration (or equivalent) by a third party or any other evidence that the law entitled the internet service provider to take as proof of copyright infringement or a reasonable likelihood of copyright infringement; and
- internet service providers would notify an account holder of any copyright infringement for which they were held responsible under the policy and provide the account holder with an opportunity to respond on a progressive basis by which the

internet service provider may in its discretion terminate the account for second and third notified infringements and should expeditiously terminate for a fourth notified infringement (in which event the account holder would be deemed to be a repeat infringer).

282 This draft industry code was never completed. Instead, carriage service providers and copyright owners made competing submissions to the Commonwealth Attorney General's Department about the regulation of use of copyright material over the internet. Both the IIA and the Australian Federation Against Copyright Theft (**AFACT**) made submissions. AFACT was constituted in January 2004 by the Motion Picture Association to protect the Australian Film Industry from copyright theft. Representatives of the IIA and AFACT also met during this period to determine whether consensus could be reached.

283 By August 2007 AFACT had concluded that the position of the IIA and its members was that no member "should be required to take any action against their customers who are engaging in copyright infringement over their networks". AFACT, accordingly, advised the IIA that there appeared to be "no utility in continuing communications with the IIA".

284 In consequence of this failed negotiation there is no industry code in respect of online copyright infringements as contemplated by the safe harbour provisions and s 101(1A)(c) of the Copyright Act. There is also no standard form repeat infringer policy which internet service providers must adopt to comply with the industry code or may adopt to ensure consistency across the industry. Instead each internet service provider wishing to limit liability under the safe harbour provisions has been left to formulate its own policy and to assess for itself whether its policy and the implementation of it satisfies the conditions of the safe harbour provisions. Similarly, no internet service provider may take advantage of compliance with an industry code for the purpose of avoiding a finding of the authorisation of copyright infringement having regard to s 101(1A)(c) of the Copyright Act.

285 Other circumstances are relevant to the appeal.

286 The proceeding from which the appeal was brought was filed on 20 November 2008. The trial judge heard the bulk of the proceeding in October and November 2009. iiNet did not dispute the fact that those to whom it provides internet access and related services have

infringed, even repeatedly infringed, the appellants' copyright. iiNet accepted also that it knew of these infringements since at least April 2009. Indeed iiNet accepted that since April 2009 it had "compelling evidence" of the infringements by reason of notices and accompanying information sent to it by AFACT on a weekly basis since mid 2008 (AFACT sent these notices to iiNet between 2 July 2008 and 12 March 2009). iiNet agreed that it could identify the account holders (or customers) on whose accounts the copyright infringements had occurred. iiNet accepted that it had both a contractual right and the technical capacity to terminate the accounts of these customers. However, apart from correspondence with AFACT, iiNet's only specific response to the compelling evidence it had of its customers infringing (including repeatedly infringing) the appellants' copyright was to forward the AFACT information to the police and advise AFACT, the appellants' representative, to do likewise.

287 Against this background, the appellants contended that iiNet authorised the infringements of their copyright. iiNet denied authorisation and contended that, in any event, it is protected by provisions of the Copyright Act (including s 112E and the safe harbour provisions) and the *Telecommunications Act 1997* (Cth). The extent but not the fact of the primary infringements was also in dispute.

288 The trial judge (*Roadshow Films Pty Ltd v iiNet Ltd (No 3)* (2010) 263 ALR 215; [2010] FCA 24) held that:

(1) Persons using iiNet's internet service had infringed the appellants' copyright in cinematographic films by making copies of films and communicating films to the public (s 86(a) and (c) of the Copyright Act respectively) (at [356]).

(2) In terms of the communication of a film to the public (s 86(c) of the Copyright Act and the definition of "communicate" in s 10(1) of that Act), those persons had:

  (a) made the film or films they downloaded "available online" once, thereby infringing the copyright in each downloaded film once only (at [290]-[300]); and

  (b) "electronically transmitted" the film or films they downloaded once, thereby infringing copyright in each downloaded film once only (at [310]-[317]).

(3) iiNet had not authorised those infringements of copyright (at [505]).

(4) By reason of ss 279 (disclosure not prohibited if by an employee in performance of duties as an employee) and 289(b)(ii) (person has consented to disclosure) of the Telecommunications Act, iiNet was not prevented by s 276 of that Act from using information that AFACT gave to iiNet about its customers infringing the appellants' copyright in cinematographic films (at [555]).

(5) iiNet had, and reasonably implemented, a repeat infringer policy in accordance with s 116AH(1) of the Copyright Act, and thus would have been entitled to the protection afforded by the safe harbour provisions of that Act if it had been found to have authorised the infringements (at [611]-[621]).

B. THE PRIMARY INFRINGEMENTS

B.1 The technology

289 The parties did not dispute the trial judge's description of the technology involved in the infringements of copyright.

290 The trial judge described the internet as a network of networks of computers. Computers in the network communicate in accordance with the internet protocol (**IP**) (at [44]). Data sent by means of the IP is broken into small packets. Sending and receiving computers are allocated IP addresses, which enable data packets to be exchanged (at [45]). Internet service providers (**ISPs**) allocate these IP addresses to customers (that is, account holders or subscribers to the ISP's service). However, the operation of routers means that each computer does not require its own IP address. A router uses one internet connection to enable all computers linked to the router to have internet access. ISPs thus also allocate IP addresses to routers. The number of computers linked to a router may be small or large (at [49]-[51]).

291 An iiNet customer on an ADSL2+ plan connects to the internet in the following way. The household computer sends data to the router, which forwards data to a modem. The modem then transmits data down the copper phone lines to a Telstra exchange. Data is sent from the exchange to an iiNet data centre and then to the rest of the world via undersea optical fibre cables (at [52]-[53]).

292 iiNet allocates dynamic IP addresses to its customers except for business plans customers who receive fixed IP addresses (at [54]-[55]). Despite the dynamic allocation of IP addresses to all but business plan customers, iiNet's systems enable it to match customers to the dynamic IP addresses (at [122]-[124]).

293 The proceeding concerns the use of the BitTorrent protocol which enables decentralised distribution of data over the internet, described as "peer to peer" communications (at [56]).

294 The BitTorrent protocol involves:

(1) BitTorrent client

1. A computer program or software which allows a person to access groups of computers sharing a ".torrent file". These groups of computers are known as "swarms". Each computer in a swarm is known as a "peer" (at [58]).

(2) .torrent file

2. A .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. This is the information necessary for the BitTorrent client to communicate with the swarm (at [61]).

(3) Hash value

3. Hash value is a means of identifying data. The piece hash value relates to a particular piece of data. The file hash value relates to the data of the file being shared by peers in the swarm. The BitTorrent client uses the .torrent file (which contains the hash values) to check the hash values of the data exchanged by peers in the swarm to ensure it is correct (at [65]-[66]).

(4) Tracker

4. The .torrent file provides a BitTorrent client with the location of the tracker. The tracker is a computer program which BitTorrent clients can contact by means of a web address. The tracker provides the IP addresses of peers in the swarm, thus enabling a BitTorrent client to participate in the swarm as a peer (at [69]).

295 There are many sources of .torrent files. Those sources are generally torrent index websites from which the .torrent file may be opened (at [68]). The user's computer then connects to a swarm of other BitTorrent users and immediately begins the process of downloading from, and uploading the file to, the users in the swarm.

296 The trial judge used an example to explain the process of downloading a file to a computer using the BitTorrent protocol:

> [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.

B.2 The infringing acts

297 The appellants used a computer program known as the DtecNet agent to identify the infringements of their copyright by users of iiNet's service. The DtecNet agent operated as a BitTorrent client. The trial judge described the process by which the DtecNet agent identified iiNet users infringing the appellant's copyright as follows (at [113]):

> (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… 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.

298 From 2 July 2008, and on the appellant's behalf, AFACT sent to iiNet on a weekly basis a "notice of copyright infringement" (the **AFACT notices**). The AFACT notices are in a standard form (other than in one respect explained below). They consist of a letter from Neil Gane, AFACT's Director of Operations, to Michael Malone, iiNet's Managing Director. The letter was delivered by hand and by email.

299 The covering email was in these terms:

> I am the Director of Operations at the Australian Federation Against Copyright Theft (AFACT).
>
> AFACT's members and their related companies are either the owners or exclusive licensees of copyright in the majority of commercially released motion pictures including, without limitation, movies and television shows. AFACT undertakes investigations and assists with enforcement of copyright in these works throughout the world.
>
> AFACT is investigating copyright infringement in Australia and evidence has been gathered regarding large scale infringement of copyright by iiNet's customers.
>
> Attached to this email is a Notice of Infringement regarding those infringements, together with a spreadsheet setting out the details of those infringements.

300 The letter was headed:

> NOTICE OF INFRINGEMENT OF COPYRIGHT

301 The letter's subject matter was identified as follows:

> UNAUTHORISED COMMUNICATION AND TRANSMISSION OF COPIES OF MOTION PICTURE FILMS AND TELEVISION SHOWS IN AUSTRALIA
> INFRINGEMENT OF COPYRIGHT IN AUSTRALIA BY CUSTOMERS OF IINET LIMITED

302 The letter of 2 July 2008, for example, was in the following terms:

> I am the Director of Operations of the Australian Federation Against Copyright Theft (AFACT). AFACT was established to protect the film and television industry, retailers and movie fans from the adverse impact of copyright infringement in Australia. AFACT acts on behalf of approximately 50,000 Australians directly impacted by copyright theft including independent cinemas, video rental stores and film and television producers.
>
> 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 … 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.

The motion pictures and television shows listed in the spreadsheet include *The Chronicles of Narnia: Prince Caspian, Juno, The Simpsons Season 19, Blood Diamond, Grey's Anatomy Season 4, Lost Season 4* and *Ugly Betty Season 2*. The titles of the files correspond to titles of motion pictures produced and distributed by AFACT's members and their affiliates. In many cases, the spreadsheet indicates that individual customers were involved in multiple infringements of copyright, making them repeat infringers. It is also likely that because the copyright material was communicated to the public that there were other infringements of copyright by customers and other internet users.

The communication to the public of the motion pictures and television shows listed in the spreadsheet took place without the license or permission of the owners of copyright.

AFACT are unaware of any action taken by iiNet to prevent infringements of copyright in movies and television shows occurring on its network of the kind identified in the spreadsheet, or to prevent customers identified as engaging in such activity, including the Identified iiNet Customers, from engaging in further infringements of copyright. The fact that iiNet customers continue to infringe the copyright of AFACT's members and affiliates suggests that iiNet has taken no action to prevent these or similar infringements from taking place.

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.
>
> This letter is without prejudice to the rights and remedies of the AFACT member companies and their affiliates, which rights are expressly reserved.

303 The letter annexed extracts from iiNet's customer relationship agreement (**CRA**) prohibiting the use of iiNet's service to commit an offence, to infringe another person's rights or for illegal purpose or practices or "allow anybody else to do so". The CRA enabled iiNet to cancel, suspend or restrict the supply of the service if, amongst other things, iiNet reasonably suspected illegal conduct by the customer or any other person in connection with the service.

304 The letter also annexed an extract from the iiNet website as follows:

> NOTE: The hosting or posting of illegal or copyright material using an iiNet service constitutes a breach of iiNet contractual obligation 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.

305 The letter enclosed a spreadsheet entitled "Summary of unauthorised Film and TV Show Transmissions" and a CD with the spreadsheet in electronic form. The spreadsheet contained numerous entries referenced by "PeerID", date and time, file name downloaded, hash, Film/TV title, studio, percentage of file shared, MB [megabytes] downloaded, percentage of file downloaded, peer host name and country.

306 As explained by the trial judge (at [115]) the PeerID is number generated by the BitTorrent client upon the program initiating. At [278] the trial judge made certain

(undisputed) factual findings in respect of the information gathered by DtecNet and given by AFACT to iiNet as follows:

> 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.

307 From 16 July 2008 the standard form of the AFACT notice was amended so as to include not only a CD containing an electronic version of the spreadsheet for the period covered by the letter, but also a DVD containing all of the data underlying the spreadsheet. The letter of 16 July 2008 also enclosed DVDs with this underlying data for the earlier letters of 2 and 9 July 2008. Other than the inclusion of the DVDs the AFACT notices sent to iiNet remained in the standard form, albeit relating to copyright infringements in the period to which the particular letter related.

308 iiNet first responded to the AFACT notices on 25 July 2008. Leroy Parkinson, iiNet's Credit Manager, sent an email to Mr Gane. The email said:

> iiNet is in receipt of your letters dated 2nd, 9th & 16th July 2008 which set out allegations that iiNet customers have infringed, by the use of the BitTorrent protocol, upon the Copyright of the Motion Picture Association ("MPA") with whom AFACT are associated. iiNet is very concerned about the allegations made in your letter and suggests that AFACT promptly direct its allegations to the appropriate authorities.
>
> In support of your allegations, you have provided data containing IP addresses, dates, time and other details which are not explained, and some of which iiNet does not recognize.
>
> Your notice makes defective references to "*…identified iiNet Customers"*. No iiNet customers are, in fact, identified by AFACT. In your attachment, IP addresses have been provided as if they were synonymous with persons or legal entities, which they are not.

> On the above basis, iiNet regrets to advise that it is unable to comply with AFACT's requirements in any way.
>
> However, in demonstrating iiNet's support for the elimination of Copyright Infringement, and to support AFACT's campaign to protect its members' rights, iiNet has passed your letter and its allegations to an appropriate Law Enforcement Agency who is better placed to assist you in pursuing offenders.
>
> Please contact the following Agency to ensure the matter is dealt with appropriately:
>
> [Contact details provided for the Investigations Manager, Computer Crime Squad, West Australian Police]
>
> Should you have any further questions, please contact the writer.

309 Mr Gane then wrote to Mr Malone (letter delivered by hand and by email) on 29 July 2008. Mr Gane's letter said:

> On 25 July 2008 I received an email from Leroy Parkinson of iiNet, who describes himself as a "Credit Manager". It is not clear to me whether Mr Parkinson is taking on the responsibility as the officer from iiNet dealing with the notices of infringement, nor whether Mr Parkinson is one of iiNet's technical employees.
>
> The notices of infringement and the attached material provide iiNet with detailed information regarding the infringements, including the dates, times and the IP addresses used by iiNet customers during the infringements. Each IP address listed in the schedule is referable to a computer and to a customer account at the relevant date and time of the infringements. Given 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.
>
> Further, iiNet itself provides its customers with an explanation as to how IP addresses are allocated (see for example http://www.iinet.au/support/general/faq/how_internet_works.html "When your computer establishes a connection to one of iiNet's dial-up access points, it is assigned an IP address, so that other computers connected to the internet can transmit information to it as required").
>
> iiNet's Customer Relationship Agreement states that "All IP addresses provided by us for your use remain our property" (clauses 5.5 and 12.5). Based on the information provided, iiNet would be able to very quickly identify the relevant customer accounts at the time the infringements took place.

310 An internal iiNet email from Mr Parkinson to Steve Dalby (iiNet's Chief Regulatory Officer) and Greg Bader (another iiNet employee) of 30 July 2008 said in respect of Mr Gane's letter:

> These guys just "don't get it". We are not obligated to do squat on their allegation. iiNet will reply accordingly.

311 On 12 August 2008 Mr Parkinson sent an email to Mr Gane. After confirming that Mr Malone had authorised him to deal with AFACT on iiNet's behalf, Mr Parkinson said:

> iiNet understands how AFACT has come to its allegation of copyright infringement based on an IP address, date & time but re-iterates that this does not identify a person at all. iiNet could not possibly know the identity of the person *who* is using any given service associated with an IP address. The service could be a shared or community terminal such as at a school or a library, an internet café, a wi-fi hot spot, the service could even be a fax machine or a printer, it may not be a computer in the sole use of an individual – Exactly *who* in any of the material provided, has AFACT identified, to direct its allegation of copyright infringement at?
>
> The vigilante approach being promoted by AFACT is rejected by iiNet Ltd. The appropriate authorities for the prosecution of offenders and imposition of penalties are not ISPs and not AFACT. iiNet will not take the responsibility of judge and jury in order to impose arbitrary and disproportionate penalties purely on the allegations of AFACT. iiNet willingly and regularly cooperate with law enforcement agencies in their prosecution of offenders. We have provided you with a reference to the appropriate authorities, which AFACT has apparently chosen to ignore.
>
> 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 the pursuit of information for AFACT. AFACT is in no position to make such a comment and it achieves nothing. If AFACT is not willing to invest its own resources to protecting its rights using the correct channels available iiNet is not going to.
>
> If AFACT have a complaint of a crime being committed, it must do like everybody else and contact a law enforcement agency to pursue the matter. iiNet have already tried to facilitate this for you by passing your complaints on to such an agency.

312 On 20 August 2008 Mr Gane wrote to Mr Parkinson. Mr Gane's letter said:

> AFACT does not think that iiNet has any doubt that its identified customers are infringing copyright in motion pictures and television shows and that it can identify the customer accounts in question based on the information AFACT has supplied now over a period of 7 weeks. During that time there have been over 5702 separate instances of infringements of copyright notified to iiNet (including significant repeat infringements). Those infringements have taken place over iiNet's network and could only continue to occur as long as iiNet provides access to those customers who are engaging in infringing activity.
>
> With this information, in addition to any other information iiNet already has, iiNet could take action to prevent the infringements from continuing. iiNet could contact each of the customers, warn them against infringement and could impose sanctions if they continue to infringe copyright using iiNet's network despite the warnings provided.
>
> As far as AFACT is aware, and your email does not indicate otherwise, iiNet has not taken any of those steps or any other step to address those infringements.
>
> AFACT hopes that this position will change and that iiNet will take steps to prevent

the infringements by its customers over its network from continuing.

313 On 29 August 2008 Mr Parkinson sent an email to Mr Gane in response to another AFACT notice in these terms:

> Further to my previous emails to you on 25th July & 12th Aug 08 (attached) iiNet has received yet another letter from AFACT dated 14th Aug 08 setting out its complaint.
>
> Again, iiNet re-iterates that if AFACT have a complaint of a crime being committed, it must contact a law enforcement agency to pursue the matter. Please contact:
>
> [Contact details provided for the Investigations Manager, Computer Crime Squad, West Australian Police]
>
> iiNet will forward AFACTs letter dated 14th Aug to the above agency on your behalf.

314 On 5 September 2008 an email from Mr Parkinson to Mr Coroneos of the IIA recorded that:

> … iiNet has responded 3 times to AFACT stating our position - but the DVDs and letters keep on-a-coming. AFACT's correspondence almost constitute spam to iiNet now.

315 This evidence, together with evidence from the cross-examination of Mr Malone and Mr Dalby, left little room for doubt about iiNet's position in respect of the AFACT notices.

316 Mr Malone accepted that the information AFACT provided in the AFACT notices (once understood by him) established that users of iiNet's service were infringing copyright of the appellants. Indeed, Mr Malone agreed that the AFACT notices constituted "compelling evidence" of such infringements (see the reasons for judgment at [172]-[180]). Mr Malone also accepted that, upon receipt of the AFACT notices, iiNet was able to match the identified IP addresses with the particular customer or subscriber account involved (using information contained in the "score" and "rumba" databases, see [509]). Mr Malone described the development of his understanding of the AFACT notices in the following exchange:

> MR BANNON: … Could you identify what it is about the [DtecNet] material you received which you say enabled you to appreciate something which rendered material reliable, which you say wasn't previously understood by you as reliable? I take it you are referring to something in the DtecNet report which is filed in these proceedings; is that correct? — There was confidential material made available to me

and to our engineers for review.

I can show you a copy of that and you can point to a paragraph which you say was the difference between making something reliable or not; is that right? — I doubt I can point to a paragraph. It was more sitting down there and fully understanding end-to-end how the DtecNet process worked, how it collected its data.

What is the specific matter? Are you able to identify a specific matter which made a difference to your understanding? — I could point to two, I suppose, that made a big difference for me. The first —

… was it the fact that DtecNet downloaded a portion of the file? — That was one of the elements.

… And the second matter – there was a second matter, as well? — Yes.

… The second matter you've identified is that DtecNet undertook this activity repeatedly over time? — Yes.

They only downloaded once from each alleged infringer, didn't they? — Yes.

And the "repeatedly over time" is a reference to what? — To verify that it wasn't just a one-off - that there wasn't necessarily a false positive. My understanding was it was done at intervals over a period of time.

… But they identified – they only downloaded once from each alleged infringer, didn't they? — Again, my understanding was it was done on multiple occasions to verify that the person was actually there, and they restricted it to a particular – restricted the number of peers, which we've seen that in court already.

That was in relation to leaving it to iiNet users? — Yes.

Well, that had nothing to do with the reliability of the outcome in your mind, did it? — I think once I stepped through and understood how it was being done and tried to consider how – other ways in which it could be mistaken or spoofed, I came to the conclusion that on balance of probabilities, it was quite a reliable way to collect the data.

… Can I show you a copy of the particulars which were provided … I can assure you these are particulars which were provided on 20 November 2008 with the commencement of the proceedings. If you turn to paragraph 69 of that, you see it says:

> *DtecNet software identified iiNet users who were making available online copies of the identified films using the peer-to-peer protocol.*

? — Yes.

… What do you point to as the basis, what piece of physical information, or information at all, do you say you can point to in support of the proposition you put forward, namely, you formed that view? — I don't have anything, simply in trying to consider how this information would be collected, that's the way I thought it was done. Between December and April I became much more informed about how this is collected.

HIS HONOUR: That's 2009? — Between December 2008 – November 20 2008

> when we got the litigation commencing up until April when we had access to the DtecNet technical information. I certainly, by the end of that period, understood exactly how this was done and what the nature of the offence was.
>
> MR BANNON: And what is absolutely clear, is it not, that you certainly didn't instruct anybody before the commencement of the proceedings to make and ask specific questions about any aspects of the collection process which you say might have been a concern? — Yes. Yes, you're correct.
>
> But you accept some questions could have been asked if you were interested enough? — I think the questions were asked in our initial correspondence with AFACT, but we didn't receive any responses.
>
> So you were familiar with the initial responses, were you? — No, now I've had a chance to review those responses.
>
> Well, the person to ask about those responses, you say, is not you because you, at the time, weren't involved in it; is that right? — Yes.
>
> That would be Mr Dalby, would it? — Yes.
>
> But you've looked at those responses and you agree they don't ask any of the specific questions which you say needed answers to satisfy you about the reliability? — Yes.
>
> And the position from iiNet, at that time, was it not, that it didn't matter what AFACT said, or what information it provided, iiNet was not going to act upon those notices by providing warnings to its customers; correct? — That's correct.
>
> No matter what answer AFACT had given to any question, that position was not going to alter, iiNet was not going to act on them in the way AFACT was suggesting; correct? — Yes, that's correct.

317 The reference to April 2009 in Mr Malone's evidence is to be understood in the context of undisputed factual findings which the trial judge made at [172]-[180] of his reasons for judgment. Noting that the proceeding was commenced on 20 November 2008, with the AFACT notices having been sent to iiNet from 2 July 2008, those findings included the following,:

(1) Mr Malone's evidence made it difficult to discern the time at which he understood the DtecNet material to be compelling evidence of iiNet users infringing the appellants' copyright (at [178]).

(2) However, it would appear that Mr Malone formed that opinion by December 2008, before receiving the affidavit of Mr Lokkegaard (the Chief Technology Officer of DtecNet) specifying the DtecNet agent's method, which was filed on 25 February 2009 (at [178]).

318 Mr Dalby gave evidence as follows in respect of his position that he would have discouraged Mr Parkinson from looking at the additional data contained on the DVDs forwarded with the AFACT notices from 16 July 2008 onwards:

> MR BANNON: Can you explain why a man who says he was concerned to understand matters, you say you didn't understand, would have discouraged your employee from looking at what you had been told was additional information? — Yes.
>
> And what is that explanation, sir? — That explanation is that in the time we received the first notification up until the subsequent letter that you referred to, we have formed a clear opinion that – I had formed the clear opinion that it was impossible for us to comply. That AFACT was asking us to take steps which we couldn't do and it mattered little how much additional information was provided to us about the nature of the headings in those spreadsheets. At a higher level we were not going to continue the work that AFACT should be taking themselves. It was not our job to do AFACTs job for it and it was therefore a waste of resources to investigate or to review minute details provided for thousands of allegations.
>
> So the position is it didn't matter whether or not they explained to you in the most minute detail, each of the matters which you say you did not understand, your position was you were not going to take any action in response to them other than forward them to the police; is that correct? — We were not going to take any action to issue notices.
>
> And, therefore, it was irrelevant, as far as you were concerned, whether or not you understood the spreadsheet; is that right? — It would help me to understand AFACTs position if it was – if the communications from AFACT were clearer, but given the position that I've just described that we were not going to send the notices, that was an intellectual curiosity more than anything else.
>
> So it was irrelevant to you to know or understand what you say you didn't understand once you had made up your mind you weren't going to act on them; correct? — I wouldn't say it was irrelevant, but it was irrelevant to the decision I'd made.
>
> Well, it was irrelevant in the sense it was going to make no difference to what the company did; correct? — At that stage I still entertained an idea that AFACT would be prepared to have discussions on the matter, and that therefore improved communication was relevant.
>
> Well, if that's right why did you – why do you say you would have discouraged Mr Parkinson from looking at the DVDs? — We didn't think it was our job to conduct AFACTs business for them and therefore it was a waste of resources to have Mr Parkinson delve any further into those DVDs.
>
> So would you agree it was irrelevant, as far as you were concerned, to attempt to understand what you say you didn't understand because it made no difference to what action you were going to take; that's right, isn't it? — At that later point in time, yes.
>
> And when you say "the later point in time" certainly by 16 July; correct? — Yes.

> So by 16 July you adopted a position where it didn't matter what additional information you got, you were not going to take a step; correct? — I wouldn't say it wouldn't matter what additional information, but it didn't appear to me that there was any additional information that would change our mind. Our position was not – was that we should not be doing AFACTs work.
>
> So there was no additional information by the time of 16 July that you felt would change the position which you had adopted, namely you were not going to do what you describe as AFACTs work; correct? — No. Can I explain? If we had received authorisation by way of a court order or some other form of authorisation, that would have changed our position.
>
> But there was no additional – just focus on my question, if you would – there was no additional information which AFACT could supply which was going to alter the steps which iiNet proposed to take so far as you were concerned? — That's correct.
>
> And so you weren't concerned to find out from AFACT any further information by 16 July, were you? — No.
>
> You agree with that? — I agree.

319 The "subsequent letter" referred to in this evidence is AFACT's letter to iiNet dated 16 July 2008.

320 At [269] of his reasons for judgment, the trial judge identified that the evidence gave rise to three classes of potentially infringing acts, being infringement of the exclusive right of a copyright owner to: - (i) make a copy of a substantial part of a film, (ii) "make available online" a substantial part of a film to the public, and (iii) "electronically transmit" a substantial part of a film to the public. Aspects (ii) and (iii) arise from the definition of "communicate" in s 10(1) of the Copyright Act and the exclusive right vested in a copyright owner by s 86(c) of that Act to "communicate the film to the public".

321 The trial judge explained the dispute between the parties about the extent, but not the fact, of the primary infringements by users of iiNet's service at [270] of the reasons for judgment in these terms:

> 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.

B.3 Make available online

322 Consistent with its position before the trial judge and the trial judge's findings (at [272]-[275]) iiNet accepted that the "overwhelming majority" of infringements shown in the AFACT notices involved 100% of the film being copied by the iiNet user and made available online. The issue between the parties was (and remains) as the trial judge put it at [275]:

> … whether one makes a film available online once, or multiple times.

323 The appellants contended that there is a separate act of making a film available online (and thus infringement of copyright) every time the film is available to the BitTorrent swarm from the computer of the iiNet customer via connection (or reconnection) of that computer to the internet. iiNet contended that the iiNet user who downloaded (copied) a film to a computer using the BitTorrent protocol made the film available online only at the completion of the act of downloading; any subsequent reconnection of that computer to the internet (whereby the film would again become available to the BitTorrent swarm) constituted the same continuing infringement.

324 The trial judge explained the potential interaction between the customer's computer, iiNet's internet service, the BitTorrent protocol and the DtecNet agent as follows:

> [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".

325 The trial judge (at [285]-[300]) rejected the appellant's contentions. The trial judge considered that the focus must be "the substantive acts of persons" and not the operation of the technology. A person acts by downloading the film. The film is then stored on the computer and made available online at any time the computer is connected to the internet. A computer may be connected to the internet by human action or by the technology connecting and disconnecting the computer by the various means the trial judge described. The trial judge also noted that the appellants' approach would make it virtually impossible to assess the number of infringements occurring, leading to "an entirely arbitrary and random result, in respect of the number of copyright infringements" (at [292]). The trial judge also considered it relevant that the concept of "making available online" contains no temporal aspect (at [293]-[294]). For these reasons, the trial judge found the appellants' approach to the number of infringements by iiNet's customers making the appellants' films available online artificial and contrary to the ordinary meaning of that phrase.

326 I have reached a different conclusion for the following reasons.

327 First, the meaning of "make available online" is not affected by the manner in which either the BitTorrent protocol or the DtecNet agent operate. I do not see the fact that these two programs, operating in conjunction, may create complex evidentiary issues as a reason to construe the statutory phrase in a manner that avoids this complexity.

328 Second, while I agree that the focus of the definition of "communicate" must be the action of a person, a person may act through the use of technology. The fact that there may be multiple disconnections and connections to the internet for technical reasons (either by a failure of technology or by design, such as the dynamic allocation of IP addresses) does not change the core means by which the evidence in the case established that iiNet's users made

the appellants' films available online. Having downloaded a film using the BitTorrent protocol, iiNet's users saved the film to their computer. They took no step to disable the BitTorrent protocol thereafter (as, had they done so, the film could not have been identified by the DtecNet agent as available to it as a peer in the BitTorrent swarm). In consequence, each and every time the user connected the computer to the internet, they made the film available online. If the operation of the technology necessarily involves other connections and reconnections to the internet, the user must be taken to accept those features as part and parcel of the overall operation of the technology they have chosen to use.

329 Third, the natural and ordinary meaning of "make available online" encompasses the provision of online access to the work in question. Online access is provided by the person acting to connect the computer, on which the film is stored and the BitTorrent protocol active, to the internet. Each time the person so acts, they make the film available online. The touchstone must be that the act of connecting to the internet is a result of the person's action. The fact that, for reasons outside that person's control, there may be multiple disconnections and reconnections does not mean that a person who stores a film on their computer for (say) a year, maintains the BitTorrent protocol in an active state on their computer (by not disabling the protocol) and connects to the internet daily, makes the film available online once only. The person makes the film available online each time he or she connects that computer to the internet. The multiple disconnections and reconnections that may occur for reasons outside that person's control may create an evidentiary difficulty. However, as noted, *prima facie* at least a person who chooses to use the technology accepts it as it is. In any event, evidentiary difficulties are routinely resolved by courts including (if need be) by recourse to the identity of the party bearing the onus of proof of any particular fact.

330 Fourth, the lack of a temporal aspect to the concept of "make available online" appears to have significance only if it is assumed that a person can make a work available online once only. If the contrary view is taken – that to make a work available online means simply to provide access to the work online – the temporal issue has no significance; the touchstone is the act of connecting the computer on which a copy of the work is stored to the internet so as to provide other internet users the opportunity to copy the work.

B.4 Electronically transmit

331 The definition of "communicate" in s 10(1) of the Copyright Act, as noted, includes the act of electronically transmitting a work. Unlike the case of communicating a film to the public by making it available online (where the evidence established that the vast majority of the infringing iiNet users had downloaded 100% of one or more of the appellants' films using the BitTorrent protocol), the electronic transmission of those films raises questions of both substantiality (s 14 of the Copyright Act) and control of content (s 22(6) and (6A) of the Copyright Act). This is because, by s 14, the doing of an act in relation to a work is to be read as including the doing of the act in relation to a "substantial part of the work". Further, by the terms of s 22(6) and (6A):

> (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.

332 In contrast to the concessions that its users had communicated the appellants' films to the public by making them available online, iiNet contended that its users had not communicated films to the public by electronically transmitting them for three reasons, as identified by the trial judge at [301] of the reasons for judgment. According to iiNet the evidence constituted by the enclosures to the AFACT notices (that is, the spreadsheets and DVDs of information collected by the DtecNet agent) did not establish: - (i) electronic transmission of a substantial part of any film, (ii) electronic transmission of any film to the public, or (iii) any communication by iiNet users.

333 The trial judge held that:

> [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.

334 The trial judge (at [317]) also held as follows in respect of the number of electronic transmissions by iiNet users:

> 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*.

335 In this appeal iiNet disputed the trial judge's conclusions at [311]-[312]. The appellants disputed the trial judge's conclusions at [317]. Given iiNet's concessions about iiNet users communicating the appellants' films to the public by making them available online, the issues in respect of those users also electronically transmitting the appellants'

films is relevant only to the question of relief, should authorisation of copyright infringements by iiNet be found.

336 iiNet submitted that because the BitTorrent protocol operates by gathering pieces of the film sought to be downloaded from many peers in the swarm, the transmission of each piece from the iiNet users was a peer to peer transaction and not a communication to the public within the meaning of s 86(c) of the Copyright Act. Further, the BitTorrent protocol operates by enabling peers to transmit pieces or fragments of a film from peers in the swarm to the person downloading the film. As such, iiNet submitted, there was no transmission of a substantial part of a film by any iiNet user; the transmission was of pieces or fragments of the film only. Similarly, having downloaded a film and made it available online an iiNet user did not transmit a substantial part of the film to the public. The iiNet user only made the film available to other peers in the swarm to obtain pieces or fragments of the film in a peer to peer transaction. Finally, iiNet submitted that the iiNet user was not making any transmission because the iiNet user who stored the film on their computer did not determine the content of the transmission. Rather, content was determined by the peer in the swarm requesting the piece of the particular film.

337 iiNet's final argument may be rejected immediately. There may be more than one person responsible for determining the content of a communication. On the evidence the iiNet users downloaded the appellants' films from the swarm using the BitTorrent protocol. The iiNet users made those films available online by storing the copy on their computers with the BitTorrent protocol activated so that the films became available on connection of the computer to the internet. By this means peers in the swarm seeking to download that film using the BitTorrent protocol could obtain by electronic transmission copies of pieces or fragments of the film from the iiNet user's computer. On the evidence, the DtecNet agent (operating as a BitTorrent client or peer in the swarm) did obtain copies of pieces or fragments of film from the computer of iiNet users by electronic transmission.

338 iiNet's submissions on this point assume that a person in the position of the iiNet user, having once downloaded a film, has no further control of or even involvement in the sharing of that film over the internet by peers in the swarm. That assumption is incorrect. The iiNet user, as the evidence from the DtecNet agent in this case proved, must have continued to

store the film on the computer, continued the active operation of the BitTorrent protocol on the computer, and either continued to connect the computer to or took no step to disconnect the computer from the internet. By taking these steps, the iiNet user is responsible for determining the content of any communication of that film (or a piece or fragment of it) to the DtecNet agent and, by inference, other peers in the swarm. The other peer requesting the piece or fragment may also be responsible for determining the content but that fact does not take the iiNet user outside the scope of the definition of "communicate" as provided for in s 22(6) and (6A) of the Copyright Act.

339 iiNet submitted that s 22(6A) is intended to clarify the construction of s 22(6). However, there is no similarity between the position of the iiNet users on the evidence in this case and a person merely clicking on a link to a webpage to gain access to it. Section 22(6A) of the Copyright Act would operate to protect the person clicking on the link from potential liability. Nothing in s 22(6A) alters the fact that the evidence established that, by their actions, the iiNet users were responsible for determining the content of all transmissions of pieces or fragments of the films stored on their computer to the DtecNet agent and, by inference, other peers in the swarm. .

340 Further, the evidence about the way in which the BitTorrent protocol and DtecNet agent operates, and the evidence provided by the operation of the DtecNet Agent, entitled the trial judge to make findings based on inference. iiNet submitted that "[t]here was no evidentiary basis for a conclusion that any particular iiNet user had shared any particular content other than the single piece identified by DtecNet". While there was no direct evidence of such sharing there was evidence which enabled (perhaps even required) that inference to be drawn. From the evidence of the operation of the BitTorrent protocol and the DtecNet agent, together with the information provided by the DtecNet agent, the inference that iiNet users had shared other content with peers in the swarm was unavoidable.

341 Nor is there substance in iiNet's submission that there was no electronic transmission of any film "to the public". iiNet accepted that communications in a closed setting may nevertheless be communications to the public if the communication occurs in a commercial context to the "copyright owner's public" (*Telstra Corporation Limited v Australasian Performing Right Association Limited* (1997) 191 CLR 140 at 155-157). iiNet submitted that

in the present case the "one-on-one" (peer to peer) exchanges did not occur in a commercial context. The iiNet user making the film available online, according to iiNet, has no commercial relationship with the peer seeking to download the film.

342 iiNet's submissions should not be accepted.

343 First, the submissions overlook the fact that the iiNet user, by storing the film on their computer with the BitTorrent protocol enabled, makes the film "available to those members of the public who choose to avail themselves of it" (*Telstra v APRA* at 156).

344 Second, the audience who receive pieces or fragments of the film the iiNet user has downloaded via the BitTorrent protocol are other peers in a BitTorrent swarm. The iiNet user too is a BitTorrent peer and, via BitTorrent, obtained their copy of the film from peers in a swarm. The setting, accordingly, is not domestic or private. It is potentially worldwide and involves all users of the BitTorrent protocol for the purpose of downloading films.

345 Third, the BitTorrent peers are all members of the film copyright owner's public because, but for BitTorrent or some other mechanism for online sharing of films, these are precisely the people from whom the appellants as the copyright owners otherwise would expect to receive payment for access to the appellants' films. In other words, the case of the communication being to the public in the present proceeding is stronger than that in *Telstra v APRA*. In the present proceeding, it is the audience themselves who would be prepared to pay for the communication. The avoidance of such payment by use of the BitTorrent protocol involves clear commercial deprivation to the appellants as copyright owners.

346 The remaining and more difficult issue is that of substantiality. The trial judge's analysis overcame this issue (and that of communication to the public) by treating the swarm as a single entity (at [312] and [315]). Given the evidence about the operation of the BitTorrent protocol the trial judge concluded as follows at [316]:

> … 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.

347 Although expressed by the trial judge as an assumption, this conclusion should be understood as an inference based on the evidence. Reading [310] with [311] confirms that the trial judge was engaged in the process of the drawing of inferences from the evidence rather than mere assumptions. The trial judge's inference, moreover, was well-founded. The evidence about the operation of the BitTorrent protocol and the DtecNet agent, as well as the information provided by the DtecNet agent, is a sufficient foundation for the drawing of this inference. The issue, however, is whether the swarm may be seen as a single entity.

348 The swarm, as the trial judge found at [58], comprises users of computers which share certain characteristics. The users' computers each have had downloaded to them the BitTorrent protocol. The users of the computers have selected the same .torrent file containing the name of the file sought, the size of the file, the hash values and the tracker location (at [61]). The iiNet users have connected to the internet (and thus to the swarm) and downloaded the pieces of the film they wish to copy from the peers in the swarm. Whilst connected, all pieces downloaded to the iiNet user also become available for uploading from that user's computer to peers in the swarm. In other words, and as the trial judge found at [312], it is the very essence of the BitTorrent protocol that each BitTorrent peer provide (or upload to other peers) as much as they take (or download from other peers).

349 The problem with the conclusion the trial judge reached from this analysis (that the swarm is a single entity so an iiNet user who had downloaded 100% of a film must also have electronically transmitted 100% of the film to the swarm), as iiNet submitted, is the language of the statute. The Copyright Act vests in the owner of copyright in a film the exclusive right to communicate the film to the public (s 86(c)). By the definition of "communicate" this means making the film available online or electronically transmitting the film to the public. By s 14 that exclusive right is not infringed unless the act is done to a substantial part of the film. In the case of the communication of a film to the public, the relevant act for present purposes is thus the electronic transmission of a substantial part of a film to the public. While the electronic transmission may be over a path (or a combination of paths), there nevertheless must be identifiable an act or acts by which a person (in this case, an iiNet user) has electronically transmitted a substantial part of one of the appellants' films to the public.

350 For the reasons already given, there is no doubt from the evidence that the iiNet users electronically transmitted pieces or fragments of films to other peers in the BitTorrent swarm. Consistent with the trial judge's inference the routine operation of the BitTorrent protocol would have ensured that the iiNet user who downloaded 100% of a film, in aggregate at least, also electronically transmitted 100% of the film to other peers in the BitTorrent swarm. The size of the piece or fragment transmitted to any individual peer, however, is unknown other than in respect of the specific transmissions to the DtecNet agent.

351 The fact that the internet itself operates by transmitting small packets of data, used by the trial judge at [314] to support his conclusions, does not obviate the need for there to be an act or acts constituting the electronic transmission of a substantial part of the film to the public for the copyright owner's exclusive right to be infringed. iiNet users who have downloaded a film using the BitTorrent protocol and stored the film on their computer without disabling the BitTorrent protocol, as the evidence established, are electronically transmitting pieces or fragments of the film to other peers in the swarm and hence to the public (in the sense of the copyright owner's public). They are not necessarily electronically transmitting to the whole swarm at any one time. The swarm, moreover, presumably changes over time. On those facts, a notional aggregation of all peers as a single entity (the swarm) does not lead to an actual aggregation of all electronic transmissions that together constitute a substantial part of the film. The electronic transmissions are from (relevantly) the iiNet user to a peer in the swarm (the DtecNet agent and, by inference, other peers in the swarm when the iiNet user is connected to the internet) of pieces or fragments of the film. Whether those electronic transmissions are of a substantial part of a film or films can only be determined by assessment of the available evidence (the information provided by the DtecNet agent). That assessment has not been conducted and thus it is not possible to conclude whether any transmission is or is not of a substantial part of a film (contrary to the trial judge's observation at [314]).

B.5 Conclusion

352 For these reasons I conclude that:

(1) The evidence established that iiNet users had made the appellants' films available online repeatedly and not once only as the trial judge found.

(2) The trial judge was correct in finding that iiNet users had electronically transmitted parts of the appellants' films to the public. However, the question whether any part so transmitted was a substantial part of the film cannot be determined by treating the peers in the BitTorrent swarm for a particular film as a single entity and thereby aggregating all electronic transmissions of a piece or fragment of a film by an iiNet user to different peers in the swarm as the (single) electronic transmission of a substantial part of the film to the public. Rather, by the ordinary process of fact finding by direct evidence (the DtecNet agent information) and inference (the operation of the BitTorrent protocol, the DtecNet agent and the content of the DtecNet agent reports) conclusions are yet to be reached as to whether any iiNet user has electronically transmitted a substantial part of any film to any peer in the swarm and thus to the public.

353 It follows from these conclusions that the appellants proved numerous primary infringements by iiNet users of the appellants' copyright in films by the users making copies of the whole of those films and communicating the whole of those films to the public by repeatedly making them 100% available online. The evidence also established that some iiNet users were repeat infringers of the appellants' copyright by these activities of copying and making films available online. The evidence proved further that iiNet users had electronically transmitted parts of the appellants' films to the public, but whether those parts constituted a substantial part of any particular film so as to infringe the appellants' copyright remains undetermined and cannot be determined as part of this appeal.

354 The next issue in the appeal is whether, as the appellants contended but the trial judge rejected, iiNet authorised those copyright infringements.

C. AUTHORISATION

C.1 The trial judge's approach

355 The trial judge (at [359]-[380]) analysed four decision in detail – *University of New South Wales v Moorhouse* (1975) 133 CLR 1, *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 220 ALR 1; [2005] FCA 1242 (***Kazaa***), *Universal Music Australia Pty Ltd v Cooper* (2005) 150 FCR 1; [2005] FCA 972 (***Cooper FCA***) and *Cooper v*

Universal Music Australia Pty Ltd (2006) 156 FCR 380; [2006] FCAFC 187 (***Cooper FCAFC***).

356 At [381] the trial judge concluded that this analysis disclosed:

> … a fundamental assumption that the alleged authoriser is the one who provided the true "means" of infringement.

357 The trial judge also concluded that cases since *Moorhouse* could be divided into two categories: "technology cases" (such as *Kazaa, Cooper FCA* and *Cooper FCAFC*) and "APRA cases" (including *Australasian Performing Right Association Ltd v Jain* (1990) 26 FCR 53 and *Australasian Performing Right Association Ltd v Metro on George Pty Ltd* (2004) 210 ALR 244; [2004] FCA 1123) (at [384]). The trial judge used this distinction to support his conclusion (at [389]) that the "technology cases":

> … display the requirement for the authoriser to have provided the 'means' of infringement even more clearly.

358 The trial judge thus posed the following question (at [400]):

> Did the respondent provide the "means" of infringement?

359 The trial judge answered this question in these terms:

> [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.

360 The trial judge then dealt with s 101(1A) of the Copyright Act. Section 101(1) and (1A) provide that:

> (1) Subject to this Act, a copyright subsisting by virtue of this Part is infringed by a person 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.
>
> (1A) In determining, for the purposes of subsection (1), whether or not a person has authorised the doing in Australia of any act comprised in a copyright subsisting by virtue of this Part without the licence of the owner of the copyright, the matters that must be taken into account include the following:
>
> (a) the extent (if any) of the person's power to prevent the doing of the act concerned;
>
> (b) the nature of any relationship existing between the person and the person who did the act concerned;

> (c) whether the person 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.

361 At [415]-[416] the trial judge said:

> [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 FCAFC*. 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.

362 The trial judge then dealt with each of the considerations in s 101(1A) of the Copyright Act.

5. (1) As to **s 101(1A)(a) (power to prevent)**: the trial judge considered that iiNet had no control over the BitTorrent system (that system being the "means" of infringement). Accordingly, "the only relevant power [iiNet] had to prevent infringement was to warn and then terminate/suspend its subscriber's account based on the AFACT notices" (at [424]). However, the trial judge concluded that "there was inadequate evidence… to make any finding regarding the scope and effectiveness of such mechanisms" (at [424]). Further, the trial judge did not consider warning and termination or suspension of a subscriber's account based on the AFACT notices to be reasonable, as iiNet did not create or control the BitTorrent system (at [436]). The trial judge also considered warning and termination or suspension a form of "collective punishment" in that the iiNet user responsible for the copyright infringement may not be the iiNet customer (at [440]). For these reasons the trial judge concluded that iiNet had "no relevant power to prevent the infringements which were occurring" (at [444]).

6. (2) As to **s 101(1A)(b) (nature of relationship)**: the trial judge acknowledged that there is a "direct relationship" between iiNet and "the owners of the accounts upon which the infringements occur", the relationship being in contract pursuant to

the CRA (at [447]). Nevertheless, because the trial judge was also satisfied that it is not "necessarily in the respondent's [iiNet's] interests to have the iiNet user's infringing" (at [452]) the contractual relationship "of itself does not persuade the court that the respondent [iiNet] is authorising the infringements of the iiNet users" (at [453]).

7. (3) As to **s 101(1A)(c) (reasonable steps)**: the trial judge repeated his earlier finding as follows (at [458]):

> 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.

363 The trial judge also dealt with iiNet's knowledge of infringements of the appellants' copyright by iiNet users (at [461]-[472]). At [465] the trial judge said:

> 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… 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.

364 At [471]-[472] the trial judge found:

> [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.

365 The trial judge synthesised the effect of these findings in the following terms:

> [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.

366 The trial judge then considered whether, in light of these findings, it could be said that iiNet had "sanctioned, approved, countenanced" its users' infringements of the appellants' copyright. iiNet conceded that the trial judge was in error at [494] by treating these terms as conjunctive rather than disjunctive, but submitted that this error was immaterial by reasons of the trial judge's subsequent finding at [501] that iiNet had not:

> … 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.

367 For these reasons, the trial judge concluded as follows:

> [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.

C.2 Reasons for a different view of authorisation

368 Five considerations lead me to a different conclusion from that of the trial judge on the question of authorisation.

369 First, although it is apparent that s 101(1A) of the Copyright Act is based on the concept of "authorisation" developed by Gibbs J in *Moorhouse*, the fundamental obligation is to apply the statute. This is apparent from s 101(1A) itself which prescribes that in determining for the purposes of s 101(1) whether or not a person has authorised any act comprised in a copyright, the nominated matters must be taken into account. The difficulty with the trial judge's approach is that, having already determined that iiNet had not authorised the copyright infringements by reference to another test (the "means of infringement" test), the trial judge then considered the required factors under s 101(1A) (at [415]-[416]). The trial judge's answers to questions posed by the other "means of infringements" test, however, determined his conclusions about the s 101(1A) factors. This is apparent from the trial judge's finding that iiNet had no power to prevent the infringements because it did not control the means of infringement (at [424] and [436]). It is also confirmed by the trial judge's statement at [447] that:

> … the mere existence of the contractual relationship, given the preceding discussion, does not persuade the court to change its finding regarding authorisation.

370 The unavoidable inference is that the trial judge considered the matters specified by s 101(1A) of the Copyright Act (that is, in determining whether or not a person has authorised any act comprised in a copyright) within and by reference to the conclusion already reached (that iiNet had not authorised the infringements of copyright) and as a result of applying a test not specified by the statute (the means of infringement test).

371 APRA, given leave to intervene for the reasons Emmett J provides, conveniently identified these issues as follows:

> (a) … the "means" represents a gloss upon the statute, which no differently from other glosses on statutory language, is not to be permitted to divert argument away from the words of the statute: cf *Fish v Solution 6 Holdings Ltd* (2006) 225 CLR 180 at [28]; *Walker Corporation Pty Limited v Sydney Harbour Foreshore Authority* (2008) 233 CLR 259 at [47].
>
> (b) Moreover, seeking to identify the "means" is an unhelpful gloss, as is made clear by the qualifications "true", "particular", "narrower" and "more specific" [see, for example, [381], [399] and [401]].

(c) … the error is with respect compounded by the reasoning at [415]. With respect, before any determination of authorisation can be made, the statute requires consideration of the mandatory considerations in s 101(1A). It is quite wrong to reason that because iiNet did not provide the "means" of infringement, it did not authorise the infringement "regardless of [the Court's] consideration of s 101(1A)": at [415].

(d) … the matters in s 101(1A)(a) and (c), namely, the power to prevent the infringing act, and the taking of reasonable steps to prevent or avoid the infringing act, make it plain that a focus on "the means" of infringement is narrower than the statutory concept of authorisation. It is plain from those paragraphs that *failure to act* can give rise to authorisation (at least where there is knowledge or reasonable suspicion of infringing conduct). That is no different from the position before s 101(1A) was enacted: see *Adelaide Corporation v APRA* at 487 and 490-491 and *University of NSW v Moorhouse* (1975) 133 CLR 1 at 12-13. An example in respect of the current form of the legislation may be seen in the reasons of Branson and Kenny JJ (with each of which French J agreed) in *Cooper v Universal Music Australia Pty Ltd* (2006) 71 FCR 1 at [41] and [148] and [155]. Yet a focus on "the means" of the infringement (at least as that term is ordinarily understood) will lead to an unduly narrow focus on the things in fact done, rather than things omitted to be done.

(e) … it is likewise wrong to consider the mandatory s 101(1A) considerations through the prism of an earlier finding that the respondent had not provided the "means": see at [424] and [436].

372 Second, and as APRA's submissions also exposed, the trial judge analysed earlier decisions for the purpose of attempting to identify a unifying principle. The trial judge applied the principle so formulated (the alleged authoriser must control the means of infringement) as exhaustive of the word "authorises" as it appears in s 101 of the Copyright Act. None of the earlier decisions identified an exhaustive test. As APRA again conveniently put it:

> The primary judge derived his emphasis on the "means" of infringement from the reasons of Gibbs J in *Moorhouse* (see especially [369] and [373]-[374]). But it is plain that Gibbs J was there identifying *sufficient* conditions for authorisation. The primary judge with respect erred in reasoning that providing the "means" was a *necessary* condition, such that the finding that iiNet had not provided the "means" of infringement was dispositive of the authorisation case.

373 Third, as a necessary prerequisite to the development of the means of infringement test, the trial judge distinguished between what he described as the "APRA cases" and the "technology cases". However, and as APRA submitted:

> At the *factual* level, there is no basis for such a distinction. APRA is inevitably engaged in technological developments impacting the performing right of the APRA Repertoire, rather than merely cases involving the "traditional" performance in public spaces (as in *Adelaide Corporation v APRA* (1928) 40 CLR 481, *APRA v*

> *Canterbury-Bankstown League Club Ltd* [1964-5] NSWR 138, *APRA v Jain* (1990) 26 FCR 53 and *APRA v Metro on George Pty Ltd* (2004) 210 ALR 244). Examples are:
>
> (a) the music-on-hold litigation culminating in *Telstra Corporation Ltd v APRA* (1997) 191 CLR 140;
>
> (b) *APRA Ltd v Monster Communications Pty Ltd* (2006) 71 IPR 212, concerning the licences granted by APRA to download ringtones to a user's mobile phone, of which, as at 30 June 2006, there were 47: see at [6]; and
>
> (c) the digital downloads determination of the Copyright Tribunal [2009] ACopyT 2 referred to more than thirty entities (notably, Apple) with licences from APRA authorising online downloading of music: [2009] ACopyT 2 at [24].
>
> More importantly, there is no *legal* basis for the distinction adopted by the primary judge. Some classes of infringing conduct involve digital technology, some do not. True it is that where digital technology is involved, it will be necessary for the Court to hear evidence and make findings as to what precisely occurs, and in particular the matters to which s 101(1A) requires the Court to have regard may involve technically complex and highly contestable issues (cf *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd (Kazaa)* (2005) 220 ALR 1 at [195]-[330]). But that is merely applying identical legal principles to different factual circumstances.

374 Fourth, assuming the "means of infringement" test to be valid, the critical role of the connection to the internet provided by iiNet to its customers (and thereby, of necessity, to users of that connection) cannot be overlooked. The trial judge found the "BitTorrent system" to be the means of infringement (for example, at [402]), yet, as the appellants submitted:

> The "BitTorrent system" includes the internet connection between the constituent parts… Without the facilities provided by iiNet, iiNet users cannot use BitTorrent to transmit or make available online the appellants' films and television programs.

375 In this regard references to "provision of the internet" (at [401], for example) and "mere use of the internet" (at [402]) tend to obscure iiNet's true function as an internet service provider.

376 As the CRA (August 2009 version) discloses, prospective customers apply to iiNet for the supply of services (cl 2.2). Available services include telephone services, voice communication services over the internet (or VoIP services), ADSL internet services (broadband internet access) and dial-up internet services. iiNet decides whether to accept the application (cl 2.4). To take ADSL internet services as an example, if iiNet accepts the application, iiNet then connects the service (cl 3). To connect the service, iiNet activates the telephone circuits on the customer's ADSL phone line (cl 3). The customer then connects

their computer to a modem and connects the modem to the ADSL phone line. If requested by the customer, iiNet provides a modem and any necessary software (section B(ii): ADSL Service Description, cll 3 and 5).

377 Under the terms of the CRA the iiNet customer or subscriber is responsible for the use of the service. Accordingly, cll 4.2 and 4.3 provide as follows:

> **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;
> (b) in any way which damages or interferes (or threatens to damage or interfere) with the operation of a Service or with the efficiency of our Network or a Supplier's Network (including because you have inadequate capacity);
> (c) in any way which makes it unsafe or which may damage any property or injure or kill any person;
> (d) to transmit, publish or communicate any material which is defamatory, offensive, indecent, abusive, menacing, threatening, harassing or unsolicited;
> (e) for illegal purpose or practices;
> or allow anybody else to do so.
>
> **Your responsibility**
> 4.3 You are responsible for and must pay for any use of the Service, including in circumstances where you have not authorised such use but such unauthorised use has arisen out of your negligent or wrongful act or omission, and you will continue to be liable for all charges relating to any use of the Service if you allow another person to occupy the Premises or use the Service. Also, if you do not disconnect the Service when you leave the Premises or transfer legal responsibility for the Service in accordance with clause 19.1, you must pay for any use of the Service by later occupants or others. Any person who uses the Service, or allows someone else to use it, after you have vacated the Premises, is jointly and individually liable with you for any charges relating to that use.

378 Clause 12.3 provides:

> **Use of your personal information**
> 12.3 We may collect, use and disclose Personal Information about you for the purposes of:
> (a) verifying your identity;
> (b) assisting you to subscribe to our services and the services of iiNet Related Entities;
> (c) providing the services you require from us and from iiNet Related Entities;
> (d) administering and managing those services, including billing, account management and debt collection;
> (e) conducting appropriate checks for credit worthiness and for fraud;
> (f) determining whether to provide to you (or to cease or limit the

provision to you of) trade, personal or commercial credit and the ongoing credit management of your account;

(g) researching and developing our services;

(h) business planning; and

(i) promoting and marketing our services, products and Special Offers to you and the products and services of Related iiNet Entities;

379 "Personal information" is defined to mean:

… 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.

380 Clause 14.2 relevantly states:

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

…

(b) you breach a material term (other than a breach which separately gives rise to rights under this clause 14.2) and that breach is not capable of remedy;

(c) you breach a material term (other than a breach which separately gives rise to rights under this clause 14.2) and, where that breach is capable of remedy, you do not remedy that breach within 14 days after we give you notice requiring you to do so;

…

(i) you breach clause 4 or clause 5.3 or your obligations relating to the use of the Service under the Service Description, or otherwise misuse the Service;

(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 our CRA;

…

381 By these arrangements iiNet provides its customers with the technology necessary to enable customers (and other users of the customer's service as expressly contemplated by the CRA) to use a computer to connect to the internet. It is by this arrangement and this arrangement alone that an iiNet customer or user of a computer can download the BitTorrent

protocol, locate and open the desired .torrent file, use the tracker to communicate with other peers, download the desired film, make the downloaded film available online and communicate pieces or fragments of the downloaded film to other peers in the BitTorrent swarm.

382 The appellants, against this background, rightly emphasised the disjunction between the trial judge's description of the use of BitTorrent in [74]-[77] of the reasons and characterisation of the role of iiNet as the internet service provider at [400]-[404]. Each of the acts described in [77] of the reasons (such as "interrogate", "request", "download", "decide", "share", "transmit", "accept" and "receive") is achieved by the iiNet customer or user connecting to the internet through iiNet's internet service.

383 I do not agree with the characterisation of iiNet's functions as the internet service provider by reference to an apparent assumption (see the reasons of the trial judge at [401]) that there can be one means of infringement only – that is, "*the* 'means' of infringement" (emphasis in original). Even if the "means of infringement" test is valid, I see no basis for requiring each alleged authorisation to disclose a single means of infringement only. The trial judge also considered that the appellants' focus on the centrality of iiNet's function incorrectly suggested that *Kazaa* was wrongly decided, as no internet service provider was joined as a respondent to the *Kazaa* proceeding (at [401]). *Kazaa*, however, turned on its own facts. That the applicant in *Kazaa* elected not to join any internet service provider as a respondent is immaterial. The present proceeding had to be resolved on its own terms and its own facts.

384 For the same reasons I do not consider that iiNet's provision of internet services may be equated to the provision of a power supply to enable the operation of facilities (at [400]). Virtually all modern equipment requires electricity to operate. The supply of power is thus a factor common to operation of most equipment. It is access to the internet, not the power enabling a computer to operate, which may or may not be capable of use to infringe copyright. In this case iiNet provided a service for the purpose of enabling (at a price) access to the internet in circumstances where it knew both that access to the internet was capable of use to infringe copyright and the internet contained copyright material. This is not the same position as a supplier of power.

385 Fifth, I cannot reconcile the trial judge's concern about "collective punishment" – which partly founded the conclusion that a scheme of notification and termination of suspension of a customer's account was not a reasonable step – with iiNet's CRA or other iiNet policies. The trial judge expressed this concern at [439]-[441], noting that in no previous proceeding had 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" (at [439]).

386 Again, the fact that similar relief had not been sought in earlier proceedings is immaterial to the question of authorisation. Nor can holding iiNet customers accountable for use by others of their iiNet service be characterised as a form of "collective punishment" not sanctioned by the Copyright Act. To the contrary, and despite its repeated reliance on the distinction between customers and users, iiNet itself holds the nominated customer or subscriber or account holder (all three descriptions being used from time to time) responsible for all uses of the iiNet service of that customer by others. Hence:

(1) By cll 4.2 and 4.3 of the CRA the iiNet customer is effectively held to be responsible for use of the iiNet service by others.

(2) iiNet draws no distinction between iiNet customers and iiNet users in its "Handling Life Threatening and Unwelcome Calls" policy. The policy, in effect, treats the iiNet customer as responsible for the use of the service so that warnings are sent to the iiNet customer on the basis of a three warnings then disconnection scheme.

(3) iiNet also draws no distinction between iiNet customers and iiNet users in its Network Abuse policy. For example, irrespective of the user, this policy assumes the iiNet customer is responsible for spam sent from the customer's IP address and reserves to iiNet the right to suspend "the offending account where necessary, or [block] their IP address from connecting".

387 Against this background, iiNet's response to AFACT that it could do nothing on the ground that IP addresses are not synonymous with persons or legal entities so that AFACT had not named any person to whom allegations of copyright infringement could be directed rings hollow. This is confirmed by iiNet's true position at the time of its response to the AFACT notices – namely, as Mr Parkinson's email of 30 July 2008 put it:

We are not obligated to do squat on their allegation.

388 For these reasons, the question of authorisation must be determined as part of this appeal.

C.3 Authorisation – matters in s 101(1A) of the Copyright Act

389 Before considering the matters specified in s 101(1A) of the Copyright Act, two preliminary comments are required.

390 The first, which arises from the above discussion about collective punishment, is that I do not accept the validity of the distinction iiNet consistently sought to draw between iiNet customers and iiNet users. As iiNet's CRA and other policies disclose, iiNet (at least in all respects other than copyright infringement) operates on the basis that the iiNet customer is taken to be responsible for the use of the customer's service by any other person. The customer is taken to be responsible not only in terms of payment but also potential sanctions for misuse of the service including warnings, suspension and termination of the service. This basis of operation, reflected in the CRA and other iiNet policies, is a practical necessity given the way in which internet access is provided. It is also appropriate to operate on that basis in the copyright context.

391 Accordingly, insofar as iiNet's case depended upon the materiality of any such distinction, it should not be accepted.

392 The second is that iNet's reliance on the provisions of the Telecommunications Act (dealt with in section D below) carries no real weight as a factor in the authorisation case. This requires further explanation.

393 iiNet relied on the provisions of the Telecommunications Act in two ways.

394 iiNet submitted that the provisions of the Telecommunications Act prevented it from taking action as sought in the AFACT notices. If iiNet could not take any action to respond to the AFACT notices then it could not be found to have authorised the infringements of copyright identified in those notices. This involves questions of statutory construction, dealt with in section D below.

395 iiNet also submitted that, irrespective of the proper construction of the provisions of the Telecommunications Act, iiNet personnel thought the Telecommunications Act prevented it from taking action. This belief (whether correct or not), submitted iiNet, is relevant to the question of authorisation.

396 It is this second aspect of iiNet's submissions which requires comment at this stage.

397 The trial judge found Mr Malone of iiNet genuinely believed that the Telecommunications Act prevented compliance with the AFACT notices though it was "unclear when such belief arose" (at [161]). The trial judge found that Mr Dalby did not have the Telecommunications Act in mind when drafting iiNet's response to the AFACT notices (at [212]).

398 iiNet's attempt to rely on the states of mind of its management about the Telecommunications Act as a factor weighing against any finding of authorisation should not succeed. It is clear from the communications identified in section B2 above that iiNet's position was that it had no obligation to do anything in respect of the information provided to it by AFACT. iiNet's responses to AFACT were formulated without any consideration of the Telecommunications Act. iiNet did not suggest to AFACT that the Telecommunications Act prevented action. In these circumstances, reliance on Mr Malone's belief (formed at an unknown time) as a factor weighing against a finding of authorisation is misplaced. His belief about the Telecommunications Act cannot be material in the authorisation context. For this reason, the proper construction of the Telecommunications Act provisions is dealt with separately from the authorisation question. My conclusions on authorisation are thus subject to any relevant operation of the Telecommunications Act.

C.3.1 Power to prevent (s 101(1A)(a))

399 There was a debate between the parties whether s 101(1A)(a) of the Copyright Act ("the extent (if any) of the person's power to prevent the doing of the act concerned") permitted consideration of the reasonableness of the exercise of any such power. The reference to "other reasonable steps" in s 101(1A)(c) arguably suggests that considerations of reasonableness are not outside the scope of s 101(1A)(a). It seems to me, however, that this debate is sterile. Section 101(1A) specifies that the matters which must be considered

include the matters in (a) to (c). Hence, the reasonableness of the exercise of any power found to exist under s 101(1A)(a) is not an irrelevant consideration. The reasonableness of the exercise of any power found to exist will often be in play. A finding of a power to prevent and its extent under s 101(1A)(a) is unlikely to be material if it is also found that the exercise of the power, to that or some lesser extent, would have been unreasonable. For these reasons, there was no material error by the trial judge in considering the reasonableness of the exercise of the powers iiNet possessed.

400 There was no dispute about the fact that iiNet had the power to identify the customer accounts related to the IP addresses provided in the AFACT notices. Further, there was no dispute about the fact that iiNet had the power under its CRA and the technical capacity to warn those customers of alleged copyright infringements and to suspend or terminate those accounts.

401 For the reasons already given above, I disagree with the trial judge's approach to s 101(1A)(a) of the Copyright Act insofar as this involved characterising the BitTorrent system as the means of infringement and the notion of collective punishment. I also take a different view of other factors relied upon by iiNet and accepted by the trial judge.

402 While iiNet may have been entitled to be "cautious" before acting on information provided by someone other than a party to the CRA (at [427] of the trial judge's reasons), the AFACT notices rose well above the status of mere unsubstantiated or unreliable allegations of copyright infringement. AFACT was an organisation known to iiNet and consulted for the specific purpose of addressing issues associated with the infringement of copyright in film and television. AFACT's members were identified in the letters to iiNet. Those members had a patently genuine interest in protecting their copyright. They were large and well-known organisations inherently unlikely to be involved in the making of serious allegations without believing they had a credible foundation for so doing (despite other detection programs used in the past being unreliable). The AFACT notices were specifically addressed from one chief executive to another and were delivered by hand and email. The notices did not make bare allegations of copyright infringement. They provided substantial supporting information which, on its face, indicated that considerable time, effort and money had been expended to provide iiNet with credible evidence of substantial and repeated copyright

infringements by persons using the service iiNet provided. The notices specifically requested that iiNet take action, including action under iiNet's CRA, to prevent the customers whose accounts were being used for these apparently widespread unlawful activities from continuing their illegal conduct.

403 Despite this, iiNet adopted and maintained thereafter a clearly stated position that the AFACT notices did not identify any actual infringing user and, in any event, that iiNet had no obligation to do anything in response. This first aspect of iiNet's position was adopted despite iiNet knowing not only that it could match IP addresses to customer accounts but also that its policies for dealing with other forms of unlawful or abusive activity assumed that it would do so and thereby hold customers responsible for all use on their accounts.

404 These considerations also undermine the significance which iiNet apparently gave to the AFACT notices containing what it described as unsubstantiated allegations. The trial judge accepted the thrust of iiNet's submission that it was "highly problematic to conclude that such issues ought to be decided by a party, such as [iiNet], rather than a court" (at [435]). One reason I take a different view is that this approach tends to nullify s 101(1A). Taken to its logical conclusion this approach means that a power to prevent will never be able to be proved in an authorisation case unless the primary infringement itself has been found by a court. Yet, if it were practical and sensible to prevent infringements by a case against primary infringers then, presumably, proving a case of infringement by authorisation would be otiose.

405 Further, the AFACT notices, on their face, provided credible evidence of widespread infringements of copyright by users of iiNet's services. The fact that iiNet did not appreciate the strength and substance of the information provided in the AFACT notices until after the commencement of the proceeding was primarily a product of iiNet's adopted position from the outset that it was not obliged to "do squat" in response. The two factors that Mr Malone said ultimately provided the compelling nature of the evidence of infringements (that the DtecNet agent actually downloaded parts of files and did so repeatedly) were apparent from the schedules and other information in the AFACT notices, had iiNet personnel bothered to analyse them. iiNet did not do so because its position was that it had no obligation to do anything in response to the AFACT notices and thus there was no point in scrutinising the

information they in fact provided. It cannot be doubted on the evidence that iiNet's position was that it need not do anything in response to the AFACT notices irrespective of the cogency of the information AFACT supplied about widespread infringements of copyright by users of iiNet's service.

406 Another reason I take a different view is that iiNet's position on the use of its service in a manner infringing copyright was not only inconsistent with its approach to other management issues (such as customers not paying bills or exceeding their quota), but also inconsistent with its approach to other types of internet abuse (such as spamming). The unavoidable inference is that when its own interests were at stake, iiNet exhibited no hesitation in: - (i) using IP addresses to identify the relevant customer accounts, (ii) treating the customer as responsible for all use of the iiNet service on the customer's account, and (iii) promulgating a regime of warnings, suspension and termination (albeit discretionary) of the customer's account. However, when its own interests were either not at stake or, at worst, might have been adversely affected by taking action, iiNet adopted a contrary position. As to its own interest, while there is no basis to question the trial judge's finding that iiNet did not necessarily benefit from its users infringing copyright (at [452]), it is not irrelevant that Mr Malone agreed that he knew both that about half of all of the traffic on iiNet's service (in terms of quota or megabytes) is via BitTorrent and a substantial proportion of BitTorrent traffic involves the infringement of copyright. This forms part of the factual context in which the issue of authorisation is to be determined.

407 I also accept the appellant's submission that the evidence of Westnet's policy of advising customers that Westnet had received notice of copyright infringements on that customer's account could not be dismissed as immaterial. The trial judge said (at [433]):

> 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…

408 I do not share this assumption. There was no evidence of the efficacy or otherwise of Westnet's policy in reducing copyright infringements. It is also difficult to accept that most people when notified of copyright infringement by them or a person using their service would simply ignore the notice unless threatened with termination. Not all people would be aware

of the risk of acting unlawfully in downloading films and television shows from the internet. Not all people would be aware that their downloading activities can be monitored both by third parties (such as copyright owners using software like the DtecNet agent) and internet service providers. When confronted by a mere notice or warning with evidence both of copyright infringement (either by them or another person they permitted to use their internet service) and the ease with which it can be detected by third parties, it is difficult to accept that there would be no deterrent effect whatsoever. To the contrary, it could readily be assumed that many people on receipt of a mere notice or warning would be deterred from future infringements irrespective of termination. The fact is that by receipt of a mere notice or warning people would realise that activities they might have thought innocent or at least undetectable were in fact unlawful and open to scrutiny.

409 The Westnet policy of notifying customers of receipt of evidence of copyright infringements on the customer's account is also important for other reasons.

410 The Westnet policy indicates that it is feasible for an internet service provider to respond to the receipt of credible evidence of copyright infringements by users of its service. The Westnet policy also indicates that there is no particular difficulty with an internet service provider holding a customer responsible for the use of that customer's service (consistent, in this case, with iiNet's CRA and other policies about internet use). iiNet's reaction to the Westnet policy is also telling. Mr Malone of iiNet, when informed about the Westnet policy, forwarded an email as follows:

> Query: what is the benefit of passing it on? For instance, what if the customer says "so what?". My general policy has been … a little less umm proactive.

411 The benefit of informing customers of the receipt of evidence of copyright infringements occurring on their accounts, as noted, is twofold. First, some will become aware that their activities are unlawful. Second, some will become aware that their activities are detectable. The idea that neither would be a material deterrent to many people is unrealistic.

412 The problems Mr Malone identified in respect of a scheme of notification and termination are also unconvincing. These problems were adopted by the trial judge at [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.

413 All of the questions posed in [434], however, are answerable. An internet service provider is confronted by precisely the same problems when dealing with spamming and other forms of internet abuse. iiNet has been able to formulate (and presumably implement) its policy for dealing with network abuse. The questions posed at [434], of course, are also those that the legislature contemplated would be addressed by the negotiation and adoption of an industry code under Pt V of the Copyright Act. It is one thing to recognise that these questions have not been answered by iiNet individually or in an industry code. It is another to assume that because they might be difficult to answer they are unanswerable or otherwise present some insuperable hurdle to an internet service provider responding to evidence of copyright infringements by users of its service, other than by simply forwarding the evidence to the police. Such an assumption, indeed, is contrary to the express intention of the legislature that answers to these types of questions be negotiated between stakeholders and documented in an industry code as provided for in Pt V of the Copyright Act.

414 The conceptual difficulty with Mr Malone's approach is exposed by the last sentence in [434]. On the basis of an unfounded assumption that customers would do nothing if told of a copyright infringement on their account, it is said that a scheme of notification would be insufficient to constitute the taking of a reasonable step to prevent the infringement. And

because that would be insufficient, it is assumed to follow that nothing reasonable can be done.

415 It follows from this analysis that I do not see the expense and complexity of implementing a policy or scheme of warnings and suspension or termination as insuperable difficulties rendering the taking of such steps as unreasonable. The trial judge considered that the complexity and expense of such a scheme "manifestly militates against the conclusion that such scheme is a relevant power to prevent" (at [435]). For the reasons given, I consider that this conclusion does not accord with either the factual reality (that iiNet was capable of implementing equivalent schemes to deal with other issues such as network abuse and spamming) or the legislative scheme (which, by the safe harbour provisions, contemplates schemes of this very kind at least for repeat offenders).

416 I also take a different view about the significance of the "robot notices". According to Mr Malone iiNet received up to 350 (presumably, automatically generated) emails a day from the United States alleging copyright infringements (at [192]). The trial judge considered that the receipt of these robot notices by iiNet was one reason to characterise a scheme of warning and suspension or termination as impractical (at [434]). Further, that the proven unreliability of other methods to detect online copyright infringements meant AFACT – to have any reasonable expectation of a response by iiNet – had to "make clear that their data was different" (at [468]).

417 The first difficulty I have in accepting these conclusions is that, as noted, there is no reason that a scheme of warnings and suspension or termination could not specify the minimum requirements for the provision of information about copyright infringement before action would be taken. In other words, working out these issues is part and parcel of the scheme itself. Moreover, and also as noted, the legislature contemplated a scheme for repeat infringers that would include termination "in appropriate circumstances" (s 116AH(1) of the Copyright Act). Precisely the same issues would need to be addressed and resolved in that context.

418 The second difficulty is that the AFACT notices are manifestly different from the robot notices. The robot notices were sent by email from the United States to the "copyright.officer@iinet.net.au". The AFACT notices were personally addressed to and

delivered by hand to Mr Malone and sent also by email from AFACT, an entity constituted and operating in Australia. The robot notices are in a standard form which is difficult to understand. The AFACT notices are written in plain English. Once scrutinised the AFACT notices provided precise details of each alleged infringement in intelligible form. The robot notices demanded action but sought no confirmation of receipt or that action had been taken. The AFACT notices sought confirmation of both. The AFACT notices referred to action being taken under iiNet's CRA. The robot notices did not. The robot notices were unsigned. The AFACT notices were signed by Mr Gane, AFACT's Director of Operations. The robot notices were each self-contained and did not constitute a meaningful chain or correspondence. As discussed below, the AFACT notices were part of a chain of communications.

419 As these factors indicate, one essential difference between the robot notices and the AFACT notices is that it may be inferred from their content and form that the robot notices were not sent in expectations of a response. The AFACT notices, in contrast, expressly sought a response. It may also be inferred that iiNet itself recognised this essential difference. There is no suggestion in the evidence that iiNet did anything about the robot notices. In contrast, iiNet replied to the AFACT notices. Mr Parkinson replied by email on 25 July 2008. This resulted in a query by Mr Gane to Mr Malone on 29 July 2008, which in turn prompted a response from Mr Parkinson to Mr Gane on 12 August 2008. Mr Gane then sent Mr Parkinson a letter of 20 August 2008 which cannot be described as a "notice" at all. This caused Mr Parkinson to respond again on 29 August 2008.

420 In other words, the AFACT notices did not stand alone as self-contained or isolated allegations of copyright infringement. They occurred in a context. They prompted a series of communications between AFACT and iiNet. They did so because they were obviously different from the robot notices.

421 The third difficulty is that iiNet's position had nothing to do with the perceived quality of the data on which AFACT relied. iiNet, as noted, considered that it had no obligation to do anything in response to the notices and acted accordingly. In so doing, iiNet refused any meaningful engagement with AFACT (whether that be about the quality of the AFACT data, the reasonable steps that iiNet had available to it or the costs of so doing). In

these circumstances, it is not clear why AFACT could have no reasonable expectation of iiNet taking action unless AFACT made clear that its data was reliable. The fact is that (for reasons already given) AFACT's data was credible on its face.

422 One other matter must be considered in this context. The trial judge, at [420]-[421], concluded that the reasoning in *Adelaide City Corporation v Australasian Performing Right Association Ltd* (1928) 40 CLR 481 supported construing s 101(1A)(a) of the Copyright Act as not encompassing "an absolute power to prevent" (at [420]).

423 In *Adelaide Corporation* at 498-499 Higgins J considered whether terminating a lease was a reasonable step to prevent an act involving copyright infringement. His Honour, at 499, described termination as:

> … 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… In my opinion, Atkin LJ [referring to *Berton v Alliance Economic Investment Company Ltd* [1922] 1 KB 742 at 759] meant just what he said – he had in his mind a power to prevent the specific act… not a power which, if exercised, would put an end to the whole relationship of lessor and lessee.

424 I do not see this observation as lending support to a construction of s 101(1A)(a) as not including an absolute power to prevent. Higgins J's observation concerned the meaning which he considered Atkin LJ had in mind when exploring the concept of "permit". Section 101(1A)(a) has to be given its ordinary meaning. The section does not refer merely to a "power to prevent" the act. It refers to "the extent (if any) of the person's power to prevent the doing of the act concerned". The words "extent (if any)" indicate that the legislature had in mind the full range of possible power – from no power to prevent at all (hence the reference to "if any") to absolute power to prevent (legally and physically).

425 It necessarily follows from this conclusion that a "reasonable step" in s 101(1A)(c) (as a matter of construction) includes the exercise of an absolute power to prevent. Whether such a step is or is not reasonable in any case will depend on the facts of that case. As a matter of statutory construction, however, s 101(1A)(a) includes an absolute power to prevent so that s 101(1A)(c) must be construed as contemplating the exercise of such a power as a reasonable step, depending on the facts of the particular case.

426 For these reasons, I consider that iiNet had available to it power to prevent the infringements. It had both the technical capacity and the contractual right to adopt and implement a scheme of warnings and suspension or termination of customer accounts. On the evidence, moreover, it had other technical capacities available to it which it routinely used in other circumstances, particularly shaping (slowing the speed at which downloading can occur) (as provided for in cll 8.3 to 8.6 of section B(ii) of the CRA (ADSL Service Description)). The trial judge concluded that there was insufficient evidence about the capacity to adopt such technical steps (at [459]). Nevertheless, it is clear from the evidence that "shaping" was not only technically feasible, but routinely used by iiNet in other contexts (see, for example, [181], [182] and [184]). Similarly, it was clear from the evidence of other iiNet policies that there was no technical or other difficulty in iiNet "tagging" a customer's account to record the giving of warnings about actual or reasonably suspected breaches of the CRA.

427 iiNet, however, made no specific responses to the AFACT notices other than the correspondence to which I have referred (stating iiNet's position and recording that it had forwarded the AFACT notices to the police).

C.3.2 Nature of relationship (s 101(1A)(b))

428 As the trial judge found, there was a contractual relationship between iiNet and its customers and a "non-contractual and more distant relationship" between iiNet and other users of a customer's account (at [447]). As to the latter, cll 4.2 and 4.3 of the CRA holds customers responsible for allowing others to use the service. Such a user must be taken to use the service subject to the same terms and conditions as the account holder. As noted, for these reasons, and given iiNet's willingness in other contexts to treat the customer as responsible for all use of the service, no material distinction can be drawn between customers and users.

429 Under the contract iiNet provided its customers with the required equipment (if requested) and made its technology available so that, by a computer, its customer (or user) could connect to the internet. The contract was commercial in nature. iiNet is in the business of providing and making money from internet services. As noted, the trial judge was not satisfied that iiNet benefited from use of the internet infringing copyright in contrast to non-

infringing use (at [451]-[452]). That does not change the fact, however, that iiNet's relationship with its customers is commercial for the purpose of iiNet making a profit from providing its customers with internet access. It also does not change the fact that iiNet knew that about half of all of the traffic on iiNet's service (in terms of quota or megabytes) is via BitTorrent and a substantial proportion of BitTorrent traffic involves the infringement of copyright.

430 The contractual relationship also provided iiNet with the right to collect and use personal information (as defined) of the customer (and thus, by necessary implication, the user as well) for administering and managing the services (cl 12.3(d)). Such administration and management must extend to ensuring that the customer (and user) comply with the terms of the CRA, including the terms prohibiting use so as to infringe another's rights or for illegal purposes or practices or to allow anybody else to do so (cl 4.2 (a) and (e)). In the event of breach or even a reasonable suspicion of illegal or anticipated illegal conduct, the CRA ensured that iiNet may, without liability, cancel, suspend or restrict the supply of the service (cl 14.2(b), (i), (j), (l) and (n)). Restricting download speeds or "shaping" would thus be permitted under cl 14.2 of the CRA.

C.3.3 Reasonable steps (s 101(1A)(c))

431 It follows from the conclusions above that the evidence satisfies me that iiNet had available to it a range of reasonable steps to prevent or avoid the doing of the infringing acts about which AFACT complained. iiNet could have adopted and implemented a general policy or a specific response to the AFACT notices dealing with all of the practical issues identified by the trial judge at [434]. The policy could have included a series of reasonable responses by iiNet to credible allegations of copyright infringement including the type of information required before action would be taken, warnings on receipt of such information to customers, the recording of warnings, shaping the customer's service as well as suspending or terminating the customer's account. The circumstances leading to shaping, suspension or termination could also have been specified in the policy and reasonably implemented.

432 iiNet did not take any of these steps. iiNet submitted, however, that it took other steps that should be considered "reasonable steps" for the purpose of s 101(1A)(c) of the Copyright Act as follows.

(1) iiNet published a webpage that, amongst other things, stated:

> NOTE: The hosting or posting of illegal or copyright material using an iiNet service constitutes a breach of iiNet contractual obligation 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.

(2) iiNet provided facilities by which copyright owners could notify it of allegations of infringement, including an email address, a fax number and an address, details of which are published on a webpage.

(3) iiNet had what it described as "systems, processes and procedures" for dealing with allegations of copyright infringement.

(4) iiNet did not block or restrict copyright owners from collecting information about iiNet customers.

(5) iiNet received thousands of robot notices, said by iiNet to contain the same information as the AFACT notices.

(6) iiNet shaped customers' accounts once the customer exceeded their monthly downloading quota.

(7) iiNet provided its services on the terms and conditions in the CRA.

(8) iiNet provided training to new employees which usually included a session on copyright on the basis that iiNet does not condone or support copyright infringement.

(9) iiNet provided training to customer service representatives working in iiNet call centres, with training material that stated:

> Troubleshooting for P2P is pretty much a non issue, the topic is completely unsupported. Most client enquiries are related to the speed of their downloads. All we can do is verify if the speed is an issue with the P2P network or with their connection to iiNet.

(10) iiNet made available to staff on its intranet materials about copyright infringement, including an article that states:

> Because of the recent implications with file sharing, it is very important to figure out what it is they are downloading. If it is illegal or even sounds like it, stay away. Troubleshooting file sharing networks and programs is unsupported.

(11) iiNet's customer service representatives communicated this position to callers.

(12) iiNet provided its Freezone service. This service enabled iiNet customers to download from legitimate sources (such as Apple iTunes, which made available 38 of the 86 films identified as the subject of primary infringements) without the download counting towards the customer's monthly quota.

(13) iiNet responded to the AFACT notices in writing:

(a) iiNet told AFACT that it did not understand the data and the data did not identify actual infringers.

(b) The AFACT notices did not specify the actions AFACT required iiNet to take.

(14) iiNet forwarded the AFACT notices to police.

433 Many of these matters must be considered in context. iiNet's specific position on the AFACT notices was that it had no obligation to take any act in response. In fact, as Mr Malone's evidence disclosed, iiNet's general position was that unless a court ordered an account to be terminated or a customer admitted copyright infringement, it would take no action to terminate an account (at [157]). Against this background, the following conclusions may be drawn about the steps on which iiNet relied for the purpose of s 101(1A)(c) of the Copyright Act.

434 As to **(1) (the copyright notice**): This is a general notice reflecting the terms of iiNet's CRA. Three matters indicate that this note is not entitled to material weight. First, although s 101(1A)(c) must encompass steps taken to prevent copyright infringement generally (in contrast to steps taken in respect of the acts alleged to have been authorised), the note operates at a high level of abstraction. It appears on a single iiNet web page which customers would have to enter in order to read. It provides no more information than that contained in the CRA. Second, when considered against iiNet's actual position in respect of copyright infringements generally (that no action would be taken against a customer without a court order or admissions) and the AFACT notices (that iiNet had no obligation to do anything in response), the note is robbed of content. Third, at least insofar as the AFACT notices were concerned, iiNet ensured that its customers knew iiNet's actual position. Mr Malone issued a press release (available for download via BitTorrent) saying:

> 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.

435 As to **(2) (the available addresses)**: The same considerations apply as in respect of (1) above. It is also relevant to iiNet's actual position that, for an unknown period, the notified email address for copyright infringements (copyright.officer@iinet.net.au) did not in fact exist. Moreover, when an iiNet network engineer discovered this to be so he noted in an internal email (presumably to the iiNet employee dealing with such communications)

> Don't know where it's gone, but could mean you've been missing crap emails about copyright for some time.

436 As to **(3) (the systems, processes and procedures)**: The systems, processes and procedures referenced are those already identified. Otherwise, the references to the evidence provided by iiNet simply note that Mr Malone dealt with allegations of copyright infringement between 1993 and 2002, Mr Parkinson from 2002 to 2006, with a Ms Moonen taking over the role of iiNet's compliance officer in 2008. This information thus adds nothing of any real weight.

437 As to **(4) (the no blocking point)**: This appears to refer to the fact that, if it wished, iiNet could implement software preventing the operation of such systems as the DtecNet agent (that is, iiNet could prevent the detection of copyright infringement online, but has not done so). Alternatively, it may refer to the fact that after becoming aware that an iiNet account had been opened by an AFACT employee for the purpose of detecting copyright infringement by iiNet users (see, for example, at [83]-[90]of the trial judge's reasons), iiNet did not terminate the internet connection to that account. It is difficult to characterise the mere refraining from taking steps to prevent copyright owners from detecting infringement online as a reasonable step to prevent or avoid the primary infringements in this case.

438 As to **(5) (the robot notices)**: Merely because iiNet received hundreds of robot notices each day and did nothing in response to those robot notices, does not mean it was reasonable for iiNet to treat the AFACT notices in the same manner. This is particularly so given the evidence of iiNet's actual position on copyright infringements as discussed above. Further, the differences between the robot notices and the AFACT notices were obvious, contrary to iiNet's submission.

439 As to **(6) (shaping)**: Again, it is difficult to see the capacity of iiNet to restrict download speeds and the fact it used this capacity in contexts other than copyright infringement as relevant. iiNet did not use shaping as a response to copyright infringements. Its position was not to do so or to do anything unless ordered by a court or in the face of customer admissions.

440 As to **(7) (the CRA)**: The same conclusions as set out above apply. The CRA terms are one thing; iiNet's actual position another.

441 As to **(8) (training)**: A stated position of not supporting or condoning copyright infringement is not the same as the taking of a reasonable step to prevent the infringement.

442 As to **(9) (call centres)**: The training provided to call centre staff includes an instruction that refers to peer to peer software but says nothing about copyright infringement.

443 As to **(10) (the iiNet policies)**: The evidence does not support the description of this information as an iiNet policy. Rather, iiNet has collected hundreds of articles and made them available to staff on its intranet, one of which (not identified as adopted as an iiNet policy in any way) deals with file sharing and contains the statement "If it is illegal or even sounds like it, stay away. Troubleshooting file sharing networks and programs is unsupported". The last sentence, as I understand it, conveys the fact that technical support for file sharing is not provided (an accurate description of iiNet's operation).

444 As to **(11) (response of customer service representatives)**: These responses are consistent with the fact that iiNet's provision of technical support to its customers does not include the technical support of peer to peer software.

445 As to **(12) (Freezone)**: The trial judge described Freezone at [181]-[191]. Having concluded 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", the trial judge said "it is likely that it would have had some such effect to that end" (at [188]). Given the trial judge's former conclusion the latter statement must be treated as speculation that Freezone might, to an unknown extent, reduce copyright infringements. Otherwise, the

availability of Freezone is subject to the same observations above about iiNet's actual position.

446 As to **(13) (response to AFACT notices)**: The substance of iiNet's response has been discussed above. On that basis I do not accept iiNet's characterisation of its response or its materiality given iiNet's actual position.

447 As to **(14) (forwarding AFACT notices to police)**: There are two problems with iiNet seeking to rely on this action as a reasonable step to prevent the primary infringements. The first is that the elements of peer to peer file sharing do not fit readily within the offence provisions of the Copyright Act. Accordingly, it is doubtful whether the criminal (as opposed to civil) law could apply. Hence, it would have been reasonably clear to iiNet that the police would have no interest in pursuing the AFACT notices. Second, iiNet's compliance officer, Ms Moonen, forwarded an email to the same police officer nominated in iiNet's correspondence to AFACT about the activities of the person who operated the DtecNet agent as follows:

> 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 and have that individual prosecuted?
> Today?
> :)

448 While the trial judge described this as showing nothing more than, perhaps, an "overly close relationship" between iiNet and the police (at [170]), Ms Moonen's email followed an internal email from Mr Malone referring to the possibility of prosecution of those attempting to detect copyright infringements (see [167]). The tenor and substance of these communications should be considered with the other evidence of iiNet's attitude to copyright infringement by users of its service, namely:

(1) The description of allegations of copyright infringement as "crap emails".

(2) The communication that AFACT just did not "get it" – "it" being that iiNet was not "obligated to do squat on their allegation".

(3) The description of AFACT's correspondence as almost constituting spam to iiNet (that is, a form of network abuse).

(4) Mr Malone's advice to Westnet that its actions (of notifying customers of copyright infringement allegations) were "doing damage to the industry and iiNet's position on this matter".

(5) Mr Malone's description of his general policy compared to that of Westnet as being:

> … a little less umm proactive.

(6) The fact that iiNet's email address for notification of copyright infringements disappeared for an unknown period, the disappearance apparently only being discovered by chance by an iiNet network engineer.

449 On the basis of these considerations, it is difficult to accept that the steps iiNet took – generally and specifically – carry much weight in the determination of the question of authorisation.

C.3.4 Interim observations

450 By reason of the AFACT notices, iiNet had evidence of widespread and repeat copyright infringements by its customers or persons its customers were allowing to use iiNet's internet service. iiNet had a range of powers available to it that it could have reasonably exercised so as to prevent the doing of the acts of primary infringement. iiNet was in a direct contractual relationship with its customers and, in all other contexts, rightly treated customers as responsible for all use of iiNet's services. iiNet's position was that it had no obligation to do anything about the acts of primary infringement and thus, apart from communicating that position to AFACT and forwarding the AFACT notices to the police, did nothing specifically responding to those notices. It did so against the background of its position on, and attitude about, copyright infringements as discussed above. It also did so against a background where it knew that half of all of the traffic on iiNet's service (in terms of quota or megabytes) is via BitTorrent and a substantial proportion of BitTorrent traffic involves the infringement of copyright.

451 Other matters must also be considered before any determination can be reached as to whether iiNet authorised the primary infringements. The first is s 112E of the Copyright Act. The second is the evidence about other relevant circumstances. The third is the provisions of the Telecommunications Act.

C.4 Section 112E of the Copyright Act

452 Section 112E of the Copyright Act is in these terms:

> 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.

453 In *Cooper FCAFC*, Branson and Kenny JJ (with whom French J agreed) considered s 112E.

454 Branson J described s 112E as qualifying the operation of s 101(1A) (at [19]). Branson J also described s 101(1A) as guiding the process by which a judgment about authorisation of copyright infringement is reached, albeit on the basis that the section did not change the meaning of "authorise" (that is, to sanction, approve or countenance) (at [20]). At [32] and [39] Branson J also expressed the conclusion that, unless enacted out of an abundance of caution, 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…".

455 Kenny J, at [168] described the operation of s 112E as follows:

> That is, if the most that can be said is that they have provided the facilities another person has used to infringe copyright, they are not to be taken to have authorised the infringement.

456 In this appeal iiNet contended that s 112E applied so that iiNet should be taken not to have authorised any of the primary infringements of copyright. According to iiNet: - (i) s 112E was introduced as part of the Digital Agenda reforms (the *Copyright Amendment (Digital Agenda) Act 2000* (Cth)), (ii) the object of that Act (as disclosed in the Explanatory Memorandum to the *Copyright Amendment (Digital Agenda) Bill 1999* (Cth)) to increase

certainty and limit liability of carriage service providers should guide the construction of s 112E, (iii) as a beneficial provision, s 112E should be construed broadly, and (iv) in consequence, a construction excluding the operation of s 112E where factual elements relevant to authorisation arise beyond the mere provision of facilities should be avoided as antithetical to the object of the section and its beneficial purpose.

457 With this in mind, iiNet submitted that "considerations of certainty and efficient operation of information technology industries will be jeopardised if all copyright owners need do to defeat reliance on s 112E is assert to carriage service providers that infringements are taking place via their facilities". Accordingly, iiNet contended that *Cooper FCAFC*, insofar as it held to the contrary, was wrong.

458 For their part, the appellants contended that the presence of s 112E in the Copyright Act meant that insofar as the pre-existing law excluded authorisation by the mere provision of facilities such law no longer applied.

459 Neither contention is persuasive.

460 The problem for iiNet's contention is the language of the section. If the conditions of operation of the section are satisfied the person is not taken to have authorised an infringement. The conditions of operation are those specified – provision of facilities for the making of a communication and use of these facilities by another. The word "merely" serves to emphasise that the section includes an exhaustive and exclusive statement of the conditions. If it cannot be said that the person provided the facilities and another person used them, and no more, the conditions are not satisfied and the section is not available. Questions of authorisation then fall to be determined under s 101(1) and (1A).

461 iiNet's submission that it could not have been intended to displace s 112E by a mere assertion to a person of infringement overlooks the fact that, if no more can be said than provided for in s 112E, the section operates as a complete exoneration – the person is not taken to have authorised infringement. If more can be said about the facts, s 112E is not engaged. There is not complete exoneration. Nevertheless, the additional circumstances do not necessarily mean that the person has authorised the infringement. Consideration will

need to be given to all of the facts to determine whether, in the light of the matters in s 101(1A), the person has authorised the infringement.

462 iiNet's submission seeks that s 112E (a section providing for exoneration) do the work of s 101(1A) (a section providing considerations relevant to any determination of authorisation). iiNet's submission is that a mere assertion to a carriage service provider of infringement cannot be sufficient to exclude the operation of s 112E. However, whether something warrants the pejorative description of "mere assertion" or not is a question of fact. The proper place for resolution of disputed factual questions is in the process of determination contemplated by s 101(1) and (1A). Section 112E, however, operates to preclude the need for any such determination. If the two conditions alone exist – provision of facilities and mere use thereof – no further inquiry under s 101(1) and (1A) is required. The person is not taken to have authorised the infringement by the existence of those two facts. It is only if other facts exist – over and above the provision of facilities and the mere use thereof – that further inquiry is required.

463 The problem for the appellants' contention is that s 112E is to be read in the context of all of the provisions of the Copyright Act, including s 101. The factors in s 101(1A) are relevant for the purpose of determining whether a person has authorised a primary infringement. The meaning of "authorise" as sanction, approve or countenance remains. Unless there is a factual finding of authorisation (in the sense of sanction, approve, or countenance), mere consideration of the matters in s 101(1A) is insufficient. This indicates that s 112E – the exclusion from s 101(1) – was not intended to change the commonly understood meaning of "authorise".

464 If it be necessary to say so, another supporting indication is that the enactment of provisions for reasons of "abundant caution" is not without precedent. The observations in *Cooper FCAFC* are precisely that – observations which do not extend to any conclusion that s 112E was intended to change the law as expressed in *Moorhouse*.

465 Section 112E, in my view, does not apply to the facts of this case. It cannot be said that the facts are simply that iiNet provided a facility for the making of a communication and a person used that facility to infringe copyright. iiNet, by reason of the AFACT notices, knew that people were using its facilities to infringe copyright. iiNet's description of this as

nothing more than an assertion of infringement is inaccurate. For the reasons already given, the communications between AFACT and iiNet meant that iiNet had credible evidence that its customers and users were carrying out widespread and repeated acts of copyright infringement using iiNet's services. But for iiNet's position that it need not do "squat" in response, iiNet would have appreciated both the full nature and extent of the infringements identified by AFACT and their *prima facie* credibility..

C.5 Other circumstances

466 The trial judge dealt with evidence about other relevant circumstances at [473]-[486] of the reasons for judgment. I deal with the same matters below.

467 It will be apparent from the discussion above that I have reached different conclusions from those of the trial judge about iiNet's knowledge. The trial judge described iiNet, by reason of the AFACT notices, as having "general knowledge" of the primary infringements but at "such a level of abstraction" to make it difficult to act on such knowledge (at [465]). However, the AFACT notices provided *prima facie* credible evidence including precise details (such as date, time, IP address, copyright material and percentage of material downloaded) of extensive infringements of copyright by iiNet customers or people customers had allowed to use their iiNet service. iiNet had no interest in "*how* such allegations came to be made" (at [467], emphasis in original) because its position was unrelated to the credibility or reliability of the evidence presented. If the infringements specified in the AFACT notices had been of any concern to iiNet, no doubt it could have sought clarification about how the allegations came to be made. Had it done so, the answer would have been the same as iiNet ultimately conceded to be the case – that the AFACT notices provided compelling evidence of the primary infringements

468 As to iiNet's failure to act (at [475]), I do not characterise iiNet's position as representing the "middle ground" of "remaining neutral". iiNet did not remain neutral. It made its position clear. It would not do anything in respect of the AFACT notices except forward them to the police. Moreover, it would continue to provide services to the customers responsible for the copyright infringements and, thereby, continue to derive income from those accounts. It would do so in circumstances where half of the traffic over its network was via the BitTorrent protocol used in the copyright infringements about which AFACT

complained. Further, iiNet not only declared its policy of doing nothing to its own customers , it also encouraged Westnet to change its policy to accord with that of iiNet on the basis that Westnet's position was damaging the industry. By so doing, iiNet did not merely remain neutral.

469 iiNet's press release (discussed at [476]-[479]) confirms that it did not remain neutral. The press release, when downloaded via BitTorrent, appeared under a comment "Not pirated in any way", which is consistent with the tenor of other internal iiNet communications about copyright infringements discussed above.

470 Consistent with the trial judge's assessment, the Golden Girls advertisement (discussed at [480]-[484]) does not seem to me to carry any real weight in the determination of the question of authorisation. Nor does any encouragement to maximise quota use (at [485]-[486]).

C.6 Authorisation determination

471 As the trial judge recorded at [464] (citing *Nationwide News Pty Ltd v Copyright Agency Ltd* (1996) 65 FCR 399; [2006] FCAFC 187 at 424):

> Knowledge 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:

472 Nevertheless, it is also apparent that "express or formal permission or approval is not essential to constitute an authorisation" (*Nationwide News* at 422 referring to *WEA International Inc v Hanimex Corporation Ltd* (1987) 17 FCR 274 at 286). Insofar as the trial judge's reasons might suggest to the contrary at [501] by the reference to the need for a "sense of official approval or favour", a different view must be taken. Further, and as Jacobs J recorded in *Moorhouse* at 21 (quoting Bankes LJ in *Performing Right Society Ltd v Ciryl Theatrical Syndicate Ltd* [1924] 1 KB 1 at 9):

> … indifference, exhibited by acts of commission or omission, may reach a degree from which authorization or permission may be inferred. It is a question of fact in each case what is the true inference to be drawn from the conduct of the person who is said to have authorized...

473 In my opinion the circumstances of this case are not equivalent to the indifference exhibited by the lessor of the hall in *Adelaide Corporation*. In that case the lessor had no control over the performance at all. The only control or power it had was to grant, not grant or terminate the lease. iiNet, through its CRA, has vested in itself control over the use of its service in accordance with the terms of the CRA. Given the continuing or ongoing nature of its service, iiNet has powers not available to the lessor of the hall in *Adelaide Corporation*. iiNet can give customers warnings, can shape their accounts, can suspend their service and can terminate their service. It can do so as it sees appropriate, without incurring liability, on the basis of even a "reasonable suspicion" of illegal conduct by a customer or any other person in connection with the use of the service (cl 14.2(j) of the CRA).

474 Further, this is not a case of mere indifference. By its responses to AFACT iiNet made its position that it would not take action clear. By the evidence of Mr Malone and Mr Dalby it was apparent that iiNet had no interest in the credibility or reliability of the information about copyright infringements with which AFACT provided it, because it had already determined its position of taking no action. By its press release of 20 November 2008 iiNet ensured that its customers knew that iiNet would not be disconnecting any services unless copyright infringement had been proven in court proceedings. By its communications with Westnet and other members of its industry organisation iiNet sought to have its position adopted by other internet service providers. Various iiNet internal communications (as discussed above) also disclosed an apparent tone and content difficult to reconcile with its stated position to AFACT that it was "very concerned" about AFACT's allegations.

475 Assessment of the matters specified in s 101(1A) of the Copyright Act (see above) weighs in favour of a determination of authorisation. So too do the other aspects of iiNet's conduct (discussed above) in the particular circumstances presented by the AFACT notices and the information they contained. The factors on which iiNet relied to defend against a finding of authorisation, in contrast, either lack weight or, assessed in the context of the overall circumstances, are unpersuasive (both in isolation and when assessed cumulatively).

476 In summary, in this case:

(1) There was a contractual relationship between iiNet and its customers by which iiNet obtained income in return for the provision of internet services.

(2) iiNet knew that the internet was used by customers to download legitimate and copyright infringing content. iiNet also knew (through Mr Malone) that peer to peer software, including BitTorrent, was frequently used for file sharing of films and television shows in a manner that infringed copyright. Indeed, Mr Malone knew that half of all of the traffic on iiNet's service (in terms of quota or megabytes) is via BitTorrent and a substantial proportion of BitTorrent traffic involves the infringement of copyright.

(3) Through its CRA, iiNet had available to it control over its customers' use of the iiNet internet service as specified in the CRA's terms. iiNet also had a range of powers available to it to prevent or avoid copyright infringements including issuing warnings, recording the issuing of warnings against customer accounts, as well as shaping, suspending or terminating accounts.

(4) iiNet received the AFACT notices over a lengthy period, in the same form from the third week. The AFACT notices contained *prima facie* credible evidence of widespread and repeated infringements of the appellant's copyright by iiNet customers and users.

(5) iiNet adopted a position almost immediately after receipt of the AFACT notices that it had no obligation to do anything in response. Despite this, it asserted to AFACT that AFACT's information did not identify customers. While this was technically accurate, it was inconsistent with iiNet's knowledge that IP addresses were sufficient for it to identify customers and its treatment of customers as responsible for all use on their account in other contexts. It was also inconsistent with iiNet's position that the reliability of the evidence was immaterial to its position.

(6) iiNet, by its press release, ensured its customers knew that their accounts would not be terminated, irrespective of the terms of the CRA, unless AFACT could prove in court the alleged copyright infringements.

(7) iiNet asked Westnet to change its position on allegations of copyright infringement to be less proactive on the basis that being proactive would harm the interests of internet service providers.

477 These circumstances support my conclusion that iiNet authorised the primary infringements of copyright. In terms of the meaning of "sanction, approve, countenance", iiNet at least countenanced the primary infringements. It tolerated, indeed permitted, those primary infringements. More than that, by its conduct in all of the circumstances identified, it moved beyond mere indifference to at least tacit approval of those primary infringements.

D. TELECOMMUNICATIONS ACT PROVISIONS

478 iiNet submitted that it could not have authorised the primary infringements of copyright because provisions of the Telecommunications Act prohibited it from taking any action in reliance on the information in the AFACT notices (for example, warning, suspending or terminating the accounts of its users who were identified in the AFACT notices as infringing the appellants' copyright).

479 The trial judge identified three relevant categories of information: - (i) the AFACT information (which provided the IP addresses, the file name, the identity of the film or television show downloaded and the time and extent of downloading), (ii) iiNet's "score" database information (which showed the customer accounts to which IP addresses were allocated from time to time) and (iii) iiNet's "rumba" database information (in effect, iiNet's billing system which contained the names, addresses and other contact details of iiNet's customers) (at [509]).

480 Although iiNet's written submissions said that the issues in the appeal did not include the trial judge's construction of s 276 of the Telecommunications Act, that is inconsistent with the fact that the proper construction of that section cannot be disregarded in resolving the operation of other provisions in dispute (ss 279, 280, 289 and 290). In any event, it is necessary to construe those provisions (which are within Pt 13 of the Telecommunications Act) in the context of Pt 13 (Protection of Communications) as a whole.

481 Pt 13 of the Telecommunications Act regulates the disclosure of certain information and documents by "eligible persons". Eligible persons include a carriage service provider (s 271(b)). iiNet is a carriage service provider and thus bound by Pt 13.

482 The scheme of Pt 13 is as follows. Div 2 of Pt 13 (in which s 276 is located) concerns "primary disclosure/use offences". Div 3 of Pt 13 (in which ss 279, 280, 289 and 290 are located) provides a series of exceptions to the "primary disclosure/use offences".

483 Section 276(1) of the Telecommunications Act is as follows:

> 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) the contents or substance of a communication that is being carried by a carrier or carriage service provider (including a communication that has been collected or received by such a carrier or provider for carriage by it but has not been delivered by it); or
> (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) if the person is an employee of a carrier or carriage service provider – because the person is employed by the carrier or provider in connection with its business as such a carrier or provider; or
> (iii) if the person is a telecommunications contractor – in connection with the person's business as such a contractor; or
> (iv) if the person is an employee of a telecommunications contractor – because the person is employed by the contractor in connection with its business as such a contractor.

484 The parties agreed that iiNet's score and rumba information was subject to s 276(1). This information, in other words, fell within s 276(1)(a)(i), (iii) and or (iv) and s 276(1)(b).

485 The appellants contended that the AFACT information which otherwise would be subject to s 276(1)(a) was excluded from that section by the terms of s 276(1)(b). Although it might initially be assumed that the AFACT information (and notices) came to iiNet's knowledge (and into its possession) "in connection with [iiNet's] business as a [carriage service] provider" (s 276(1)(b)(i)), the appellants identified matters supporting a contrary conclusion.

(1) If the mere receipt of information or a document (in this case, collected by a third party from publicly available data on the internet) by a carriage service provider is not outside the scope of the phrase "in connection with the person's business as such a …

provider" then there is an absurd consequence. Every person other than the carriage service provider would be free to disclose or use the information or document, but the carriage service provider would be bound not to do so.

(2) Nothing in s 276(1) suggests that it was intended that information or a document obtained by a third party and provided to a carriage service provider (even if it be information or a document about the provider's business) alters its character by reason of the mere fact of provision by the third party to iiNet.

(3) An alternative construction of s 276(b)(i), insofar as it uses the phrase "in connection with the person's business as such…", is reasonably open on the language and is consistent with the evident purpose, object and scope of the section.

(4) The section is intended to protect information or documents which come to the knowledge or into the possession of the eligible person in the actual course of their operations as an eligible person (or, to adopt the appellants' description, information or a document acquired by virtue of the eligible person being in a position peculiarly to acquire information of that type). It is not intended to protect information or documents which a third party has obtained from sources other than the actual course of the eligible person's operations as such and has provided to the carriage service provider.

(5) The text of s 276 reasonably accommodates this construction. The words "in connection with" must be given a meaning having regard to the context and purpose of the section. The phrase "the person's business as such a … provider" is part of this context. The words indicate that the information or documents in question are information or documents acquired through or in the course of the eligible person carrying out its business as such (that is, its business as the eligible person).

486 The appellants' submissions about the proper construction of s 276(1)(b)(i) are persuasive. They accord with the orthodox tenets of statutory construction. iiNet's approach, in contrast, gives the language of s 276(1)(b)(i) its literal meaning without due regard to the context and purpose of the provision. Construing s 276 in the manner for which iiNet contended would lead to absurd results. It would expose eligible persons to criminal sanctions merely for disclosing or using a document that a third party had obtained from sources other than the operations of the eligible person and provided to the eligible person.

For example, if iiNet's construction were correct, iiNet presumably contravened s 276(1) (and thereby committed an offence) merely by forwarding (and thus disclosing) the AFACT notices to the police.

487 For these reasons I accept the appellants' submission that Pt 13 of the Telecommunications Act does not apply to the AFACT notices or information they contained. However, as will be apparent from these reasons, iiNet could not identify customer accounts from the AFACT notices alone. iiNet needed to use its score and rumba databases to do so. The information in those databases is subject to s 276(1) of the Telecommunications Act. Accordingly, it is necessary to consider the exceptions in Div 3 of Pt 13.

488 Section 279(1) of the Telecommunications Act provides an exception to s 276 in the following terms:

> 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) a carrier; or
> (ii) a carriage service provider; or
> (iii) a telecommunications contractor; and
> (b) the disclosure or use is made in the performance of the person's duties as such an employee.

489 The trial judge found that iiNet's use of its score and rumba information would be within the scope of s 279(1) (at [529]-[532]). I consider iiNet's submissions to the contrary persuasive. Construed in context, s 279 provides a series of exceptions from liability for employees and contractors of a carriage service provider who disclose or use information or a document protected by s 276 in the performance of their duties as an employee or contractor. Section 279 says nothing about a carriage service provider itself, such as iiNet, disclosing or using information or documents protected by s 276.

490 The fact that iiNet acts through its employees is not the point. If iiNet used its score and rumba information to disclose information about its customers, s 279(1) would ensure that iiNet's employees could not be liable for performing duties in that regard. Section 279(1) would not protect iiNet itself from liability. iiNet would have to rely on

another provision to authorise its actions. Construed as the appellants submitted, the exception in s 279 would consume the obligation in s 276.

491 Section 280(1) of the Telecommunications Act is in these terms:

> Division 2 does not prohibit a disclosure or use of information or a document if:
> (a) in a case where the disclosure or use is in connection with the operation of an enforcement agency – the disclosure or use is required or authorised under a warrant; or
> (b) in any other case – the disclosure or use is required or authorised by or under law.

492 The appellants submitted that iiNet was able to use its score and rumba information because such disclosure or use was "required or authorised by or under law" (s 280(1)(b)). According to the appellants this follows from s 101(1A)(c) and s 116AH(1) of the Copyright Act. Section 101(1A)(c) makes the taking of reasonable steps to prevent or avoid copyright infringement a relevant consideration in determining whether a person has authorised the infringement. Section 116AH(1) provides a carriage service provider with limitations on liability if the provider has adopted and reasonably implemented a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers. The appellants submitted that a carriage service provider, thereby, must be able to disclose or use information subject to s 276 at least insofar as necessary to bring itself within ss 101(1A)(c) and 116AH(1) of the Copyright Act. If it were otherwise those provisions, including s 116AH(1) (specifically addressing the liability of carriage service providers), would be nugatory.

493 I accept the appellants' submissions at least insofar as they concern s 116AH(1) of the Copyright Act. The safe harbour provisions in Pt V of the Copyright Act are specifically intended to limit the liability of carriage service providers for copyright infringements. Carriage service providers must satisfy certain conditions in s 116AH before they are entitled to the limitations. It follows that carriage service providers must be "authorised by or under law" to take such action as is reasonably necessary (including the disclosure and use of information and documents subject to s 276 of the Telecommunications Act) to bring themselves within the protection given by Pt V of the Copyright Act.

494 Because one of the conditions in s 116AH(1) is the adoption and implementation of a repeat infringer policy as described, iiNet must have been authorised by law to disclose and use its score and rumba information insofar as reasonably necessary to enable it to adopt and implement such a policy.

495 It also follows that, if (contrary to my conclusion), the AFACT notices are not excluded from Pt 13 of the Telecommunications Act by s 276(1)(b)(i) then the same considerations enabled iiNet also to disclose and use those notices which were provided to iiNet for the specific purpose of putting it on notice of repeat infringers of copyright.

496 iiNet's submissions to the contrary would undermine the operation of the safe harbour provisions. Those submissions also failed to recognise that disclosure or use merely "authorised by or under law" is sufficient to engage s 280(1)(b). It may be accepted that s 116AH(1) does not "require" a carriage service provider to disclose or use information necessary to adopt and implement a repeat infringer policy. The section, nevertheless, must be taken to authorise a carriage service provider to do so. If this were not so, the safe harbour provisions could not fulfil their intended purpose. They would be rendered futile. This cannot have been intended. The statutes are products of a single legislature. They should be construed so as to achieve a rational scheme for carriage service providers.

497 For these reasons, s 280(1)(b) of the Telecommunications Act operated to enable iiNet to disclose and use its score and rumba databases (with the AFACT notices) to take any of the various steps available to it, such as warning customers about infringing activities on their accounts, shaping of customer accounts, as well as suspending or terminating those accounts as part of any repeat infringer policy iiNet considered it appropriate to adopt and implement.

498 Section 289 of the Telecommunications Act provides that:

> 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.

499 The appellants submitted that s 289(b) was engaged (their primary argument relating to s 289(b)(ii) whilst also relying, if necessary, on s 289(b)(i)).

500 iiNet first contended that s 289 could not apply because the AFACT notices included information (for example, movie title information) that falls outside the meaning of s 289(a).

501 I do not accept this contention. The movie title information identified in the AFACT notices (assuming, for this purpose and contrary to my conclusion above, that these notices are subject to s 276) was information about the films iiNet customers or users had downloaded and shared online. As such, it was information relating to the affairs (if not the personal particulars) of those persons. The context provides no basis for reading s 289(a) down. Such information is within the scope of s 276(1)(a)(i) and (iv) (at least on the facts of this case). Contrary to iiNet's submission, there is no sound reason to read s 276(1)(a)(i)-(iv) as mutually exclusive. Information or documents may engage the operation of one or more of these subsections. It thus does not follow that information or documents within s 276(1)(a)(i) cannot also be within s 276(1)(a)(iv). Hence, s 289(a) (which repeats the language of s 276(1)(a)(iv)) should not be read as necessarily excluding information or documents which might also be within s 276(1)(a)(i), (ii) or (iii).

502 For these reasons the appellants' submissions should be accepted. The whole of iiNet's score and rumba information is within the scope of s 289(a). If (contrary to my conclusion) the AFACT notices and information they contained are subject to s 276(1), then they too are within the scope of s 289(a).

503 I am also satisfied that iiNet customers and users consented to the disclosure and use of all of this information by iiNet in the circumstances concerned as specified in s 289(b)(ii). They did so because of the terms of the CRA. iiNet's arguments that s 289(b)(ii) requires a more specific consent to the particular use proposed and that mere users (as opposed to customers) are not parties to the CRA are unpersuasive.

504 Section 289(b)(ii) requires consent to the disclosure or use in the circumstances concerned. Under cl 12.3(d) of the CRA iiNet is able to use and disclose personal information (as defined) for the purpose of administering and managing the services provided. Under cl 14.2 iiNet is able to take action to cancel, suspend or restrict the supply of the services for breach of a material term (cl 14.2(b)), for breach of cl 4 or other misuse of the service (cl 14.2(l)), if iiNet reasonably suspects fraud or other illegal conduct by the customer or any other person in connection with the service (cl 14.2(j)), if providing the service may be or iiNet anticipates it may become illegal (cl 14.2(n)) or if iiNet is allowed to do so under another provision of the CRA (cl 14.2(r)). All of these circumstances – and their investigation and resolution by iiNet – involve the administration and management of the services as specified in cl 12.3(d). iiNet can thus use "personal information" as defined for any of these purposes. Insofar as information is not personal information, as defined, the CRA provides no restriction on disclosure or use by iiNet. Customers using iiNet's service must be inferred to have consented to iiNet using and disclosing such non-personal information insofar as it is available to iiNet by reason of the customer's decision to use iiNet's services.

505 It follows that customers, by entry into the CRA, consented to iiNet disclosing and using information, including personal information as defined, for the purpose of iiNet administering and managing the services provided pursuant to the CRA. Part of that administration and management includes compliance with the CRA. In circumstances where iiNet has received evidence of breaches of its CRA (for example, cl 4.2(a) and (e)) the customer has necessarily consented to iiNet using information it possesses, including personal information, to determine whether to take action under cl 14.2 of the CRA.

506 If there were any doubt about this conclusion, the doubt is removed by cl 4.4 of the CRA which is in these terms:

> **Interception**
>
> 4.4 You acknowledge that we may be required by Law to intercept communications over the Service and may (but are not obliged to) monitor your usage of the Service and communications sent over it for the purposes of ensuring your compliance with our CRA and our compliance with the law, and with any request or direction of a Regulatory Authority, a Law Enforcement Authority or other authority. In this regard the terms of our privacy policy are also enforced. The privacy policy is located on our website for your reference.

507 By cl 4.4 iiNet customers must be taken to have consented to iiNet using information in its possession, including personal information, to enable it to monitor use of the service. In context, "your usage of the service" must mean any use of the service on that customer's account.

508 Users of iiNet's service are not in a different position from customers. A user, by the mere act of use on the customer's account, must be taken to have accepted the same terms and conditions as the customer. A user cannot be in any position better than a customer. This legal position is reflected in cl 4.2 of the CRA which makes customers liable for use of their service by another person. Moreover, and as the appellants submitted, a user is using a customer's account. Anything to do with that account involves the affairs of the customer.

509 Section 289(b)(i) is also engaged. In circumstances of a person using their internet service to download copyright material (whether or not aware of the law of copyright) the person must be reasonably likely to have been aware that their internet service provider, in the ordinary course of managing the provision of the service, would use information or documents enabling the provider to take any action it was authorised to take by the terms on which the service was provided.

510 For these reasons s 289 of the Telecommunications Act also ensured that iiNet was able to use and disclose the score and rumba information (as well as the AFACT notices) to take any of the actions available to it in respect of the primary infringements.

511 The same considerations apply to s 290 of the Telecommunications Act, which is as follows:

> 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.

512 Consistent with the reasoning above the terms of s 290(a) (which are the same as s 276(1)(a)(i)) should not be read as necessarily excluding information or documents also

within s 276(1)(a)(ii)-(iv). As discussed, s 276(1)(a)(i)-(iv) are not mutually exclusive. One or more of the subsections may apply to the same information or document. Accordingly, it is not the case that s 290(a) is incapable of applying to iiNet's score and rumba information or the AFACT information (if the latter is within the scope of s 276 at all). Taken together, that information relates to the contents or substance of a communication made by another person (namely, communications between the iiNet customer or user and the person using the DtecNet agent). Section 290(a), therefore, is satisfied.

513 Section 290(b) is also satisfied. iiNet customers (and thus users of a customer's account) use the iiNet service subject to the terms of the CRA. Clause 4.4 of the CRA constitutes consent to the disclosure or use of information relating to the contents or substance of the communications in question. The clause involves an acknowledgement by the customer (which must also bind a person using the customer's service) that iiNet may monitor use for purposes including compliance with the CRA. By reason of cl 4.4 persons using iiNet's service to download and share films and television shows in breach of copyright (and thus in breach of iiNet's CRA) must be taken to have consented to iiNet disclosing or using that information for the purpose of ensuring compliance with iiNet's CRA.

514 iiNet's submission to the contrary should not be accepted. iiNet argued that persons willing to misuse its service could not be reasonably expected to consent to the use of information proving their own misuse. This overlooks the operation of cl 4.4 of the CRA. Users of the service have consented to iiNet monitoring their communications for the purpose of ensuring compliance with the CRA. Using the service to infringe copyright contravenes the CRA. Hence, the mere assumed desire of users of iiNet service to avoid detection of their activities infringing copyright is immaterial. They use the service subject to the terms and conditions which iiNet, as the provider of the service, has imposed.

515 For these reasons, iiNet cannot rely on s 276 of the Telecommunications Act as a defence to the appellants' authorisation case. Sections 280, 289 and 290 of the Telecommunications Act applied with the consequence that iiNet, if it wished to do so, could have used its score and rumba information, as well as the AFACT notices to take whatever action iiNet saw fit under its CRA.

E. SAFE HARBOUR PROVISIONS

516 The appeal raises two issues about the safe harbour provisions in Pt V of the Copyright Act.

517 First, whether (as the trial judge found) iiNet satisfied condition 1 of item 1 of s 116AH(1) of the Copyright Act that:

> The carriage service provider must adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers.

518 Second, whether (as iiNet contended and the trial judge rejected) the "accounts of repeat infringers" refers only to account holders who are repeat infringers, not accounts used for repeated infringements.

519 In [612] of the reasons for judgment the trial judge found that iiNet had adopted a policy as required, having regard to the notice on the website (see [612] of the reasons for the full text of this notice), the CRA and Mr Malone's oral evidence (see [613]-[614]).

520 The reason I take a different view of the effect of this evidence is that condition 1 of item 1 of s 116AH(1) requires the policy to provide for termination, in appropriate circumstances, of the accounts of repeat infringers. It is one thing to advise customers that infringing copyright is a breach of the CRA which may result in termination of the service and to include provisions to that effect in the CRA. It is another to have adopted a policy that "provides for" termination, in appropriate circumstances, of the accounts of repeat infringers. To answer the latter description there must be evidence of the adoption of such a policy or evidence from which an inference of adoption of such a policy can be drawn. To be a policy as described, the policy (whether it be in writing or not) must not only provide for termination generally (such as in the notice or CRA on which the trial judge relied). It must provide for termination, in appropriate circumstances, of the accounts of repeat infringers. In other words, irrespective of the language used, the policy must in some way deal with the concepts of both "appropriate circumstances" (for termination) and "repeat infringers". Neither the copyright notice nor the CRA deal with either concept in any way.

521 As to Mr Malone's oral evidence (see [613]-[614] of the reasons for judgment), it is true that a contract may evidence a policy. In this case, however, the CRA did not evidence a policy of the required type. Moreover, the trial judge appears to have accepted that iiNet's policy existed only in Mr Malone's mind, although Mr Dalby was found to be aware of Mr Malone's state of mind (at [614]). The policy in Mr Malone's mind was to terminate accounts in three circumstances – a court order to do so, an admission of infringement by an iiNet user, and where infringement was found by a court to have been proved. However, analysis of the oral evidence on which the trial judge relied (at [614]) does not support the conclusion that iiNet adopted any policy of the requisite kind. To the contrary, it is clear from his description that no policy had been adopted. This is the only basis for Mr Malone's evidence that "we don't have a written policy… but my position would be…" and "The policy would be…". This evidence does not indicate the adoption by iiNet of a policy of the necessary kind. It discloses Mr Malone formulating, at the time of cross-examination, what he considered iiNet's policy would be if the conditions identified were satisfied. Section 116AH(1), however, required iiNet to have adopted the policy at the time of the copyright infringements (see s 116AG(1) and (3) of the Copyright Act).

522 Apart from the lack of adoption of a policy, it is also apparent that Mr Malone's oral evidence does not support the existence (even in Mr Malone's mind) of a policy of the required description. The three circumstances in which Mr Malone said iiNet would terminate an account have nothing to do with repeat infringements or repeat infringers. While Mr Malone said iiNet would need to take action if someone was found to repeat an infringement, this does not evidence adoption of a policy as described.

523 The other evidence on which iiNet relied in its written submissions does not lead to any different conclusion. The issue is adoption of a policy within the meaning of condition 1 of item 1 of s 116AH(1) of the Copyright Act. Attendance at industry information sessions about the safe harbours regime which refer to the need to adopt such a policy does not prove that a policy was adopted. Nor does an internal review of the checklist provided by the IIA to its members including iiNet (particularly where point 1 on the checklist is the need for the carriage service provider itself to adopt a policy as described in the statutory provision). The documents in respect of the development and claimed adoption by Mr Malone of an internal guide to the safe harbour provisions, on analysis, confirm that no policy was adopted.

Mr Malone said employees were seeking guidance about how they could stay within the safe harbour provisions. Mr Parkinson responded that he had drafted a document based on the IIA presentation. This document recorded the need for a policy to be adopted as a general requirement but did not set out or propose any such policy. Instead, the document summarised the statutory conditions and requirements for the various categories of activities. Mr Malone's evidence was that he "understood that [he] had approved that policy". However, that does not assist for two reasons. First, the document contains no policy of the required kind. Second, Mr Malone's understanding does not prove adoption by iiNet. Further, and in any event, Mr Malone said he did not think the document was that useful for customer service representatives who were the focus of his initial inquiry. Nor do any of the other matters to which iiNet referred (seeking advice about its CRA, redrafting its CRA, discussing the legislation at internal meetings and the like), on analysis, support any inference of adoption of a policy as referred to in condition 1 of item 1 of s 116AH(1) of the Copyright Act.

524 For these reasons, the requirement in s 116AG(1) of the Copyright Act ("a carriage service provider must satisfy the relevant conditions set out in Subdivision D before the limitations in this section apply") was not met. iiNet thus is not entitled to rely on the limitation of liability in s 116AG(3) (the relevant provision, as the copyright infringements occurred in the course of Category A activities – see s 116AC).

525 I also do not accept iiNet's construction of the phrase "accounts of repeat infringers". Only customers or subscribers have accounts. Persons who use an iiNet service will be either the customer or a person whom the customer has allowed to use their service. A carriage service provider can terminate a customer's account. A carriage service provider cannot prevent a customer from allowing a person to use the customer's service. A carriage service provider also cannot know whether the user of the service is the customer or a person the customer allowed to use the customer's service. This is the context in which condition 1 of item 1 of s 116AH(1) was formulated. In this context it is irrational to construe the condition as requiring the carriage service provider to adopt a policy that deals only with an account holder who is themselves a repeat infringer. The condition requires a policy dealing with termination of the "accounts of repeat infringers". In context, this must mean accounts in respect of which repeat infringements have occurred.

526 This reading of condition 1 does not offend any principle of statutory construction. It is merely to give the phrase "accounts of repeat infringers" meaning in the actual context of the condition as a whole and the reality in which the condition operates. In substance, iiNet's argument is another variation of the distinction it consistently sought to draw between customers and users. That distinction has no valid basis in any of the contexts on which it was sought to be introduced, including condition 1 of item 1 of s 116AH(1). Indeed, in the context of condition 1 (which includes the fact of the nature of the service provided and the ways in which that service operates) the natural and ordinary meaning of the condition is accounts of repeat infringers in the sense of accounts used for or accounts on which there has taken place repeat infringements. In any event, in the context of cl 4.2 of iiNet's CRA, "accounts of repeat infringers" would include any use made of an account – the customer who has allowed the infringing use would themselves be a "repeat infringer" for the purposes of condition 1.

F. CONCLUSIONS

527 For the reasons set out above I am satisfied that the appeal should be allowed. In summary:

(1) The appellants proved the primary infringements as identified in these reasons.

(2) iiNet authorised the acts constituting the primary infringements as provided for in s 101(1) of the Copyright Act.

(3) iiNet is not entitled to rely on provisions of the Telecommunications Act to defend itself from liability.

(4) iiNet is not entitled to rely on the safe harbour provisions in Pt V of the Copyright Act to limit its liability.

528 Therefore, the appeal should be allowed and the matter remitted to the trial judge for the determination of quantum. The appellants should have their costs of the appeal.

I certify that the preceding two hundred and fifty-four (254) numbered paragraphs are a true copy of the Reasons for Judgment herein of the Honourable Justice Jagot.

Associate:

Dated: 24 February 2011

IN THE FEDERAL COURT OF AUSTRALIA
NEW SOUTH WALES DISTRICT REGISTRY
GENERAL DIVISION **NSD 179 of 2010**

ON APPEAL FROM THE FEDERAL COURT OF AUSTRALIA

BETWEEN:	**ROADSHOW FILMS PTY LIMITED (ACN 100 746 870)** **First Appellant**
	THE PARTIES IN THE ATTACHED SCHEDULE 1 **Second Appellant to Thirty-Fourth Appellant**
AND:	**IINET LIMITED (ACN 068 628 937)** **Respondent**
JUDGES:	**EMMETT, JAGOT & NICHOLAS JJ**
DATE:	**24 FEBRUARY 2011**
PLACE:	**SYDNEY**

REASONS FOR JUDGMENT

NICHOLAS J

INDEX

INTRODUCTION

529 There are thirty-four appellants to this appeal. They include the major motion picture studios (Universal Studios, Paramount Pictures, Warner Bros, Disney, Columbia Pictures, Twentieth Century Fox) and various other entities that are the owners or exclusive licensees of copyright in thousands of commercially released cinematograph films. The respondent to the appeal (**iiNet**) is an internet service provider (**ISP**) that has carried on business in Australia since 1995. It is now a public company listed on the Australian Stock Exchange and the third largest ISP in Australia with approximately 490,000 subscribers.

530 The appellants, who were the applicants below, commenced a proceeding against the respondent for copyright infringement which was dismissed by the primary judge after a lengthy trial: *Roadshow Films Pty Ltd v iiNet Pty Ltd (No 3)* (2010) 263 ALR 215 (Cowdroy J). The appellants have appealed against his Honour's order dismissing the proceeding.

531 At the trial, the appellants alleged that the respondent infringed their copyright in 86 different films (referred to by the primary judge as the "identified films") by authorising acts of infringement committed by iiNet users. The 86 films were a small sample of films drawn from the appellants' extensive catalogues. It was admitted by the respondent that each of the 86 films was a cinematograph film in which copyright subsisted. It was also admitted that copyright in the identified films was owned by, or exclusively licensed to, one or more of the appellants.

532 The appellants alleged that iiNet users infringed copyright by communicating the films to the public by making copies available online and by electronically transmitting copies on the internet using peer-to-peer file sharing technology known as BitTorrent.

533 The respondent admitted that iiNet users had infringed copyright in the films by making them available online but argued that in every case where an iiNet user had made a film available online, he or she had done so only once. The respondent did not admit that iiNet users had electronically transmitted a substantial part of any such film or that any electronic transmissions, if made, were made to the public. The respondent denied that it authorised the iiNet users' acts of infringement.

534 On the matter of primary infringement, the primary judge found that iiNet users had made certain films available online and that they had therefore infringed copyright by communicating those films to the public. His Honour also found that in each case the film was made available by the iiNet user concerned only once. His Honour also found that iiNet users electronically transmitted certain films and had therefore infringed copyright by communicating those films to the public. Again, his Honour held that each of the iiNet users electronically transmitted the film but that each of them did so only once.

535 The primary judge then turned to the issue of authorisation and found that none of the primary acts of infringement was authorised by the respondent.

536 The appellants say that his Honour should have found that the iiNet users engaged in repeated acts of copyright infringement by both making available online and by electronically transmitting the films without the appellants' consent and that his Honour should have found that these acts of copyright infringement were authorised by the respondent.

537 The critical issue in the appeal is whether the primary judge was in error in holding that the acts of infringement by iiNet users which his Honour found to have occurred (at least some of which were admitted) were acts that the respondent had not authorised within the meaning of s 101 of the *Copyright Act* 1968 (Cth) (**the Act**). There are a number of related issues of statutory construction that are closely bound up with that issue.

538 The first concerns the meaning and effect of various provisions of the *Telecommunications Act* 1997 (Cth) (**the Telco Act**) which, the respondent argued, prevented it from taking the steps which the appellant alleged the respondent ought to have taken if it was to escape a finding of authorisation. The primary judge rejected the respondent's argument on this point. This aspect of his Honour's decision is taken up in a notice of contention filed by the respondent in the appeal.

539 The second concerns the meaning and effect of s 112E of the Act. The primary judge held that, in light of other findings made by him, s 112E would not have protected the respondent against a finding that it authorised the infringing acts of iiNet users, though, this made no difference to the ultimate result because his Honour concluded that there was no authorisation independently of s 112E. However, the respondent contends that the primary

judge's interpretation of s 112E was wrong and that, even if his Honour was otherwise in error in holding that it did not authorise the primary infringements, s 112E is still a complete answer to the appellants' claims. This is another matter which the respondent has raised in its notice of contention.

540 The respondent also relied upon the "safe harbour" provisions found in Division 2AA of Part V of the Act. The primary judge stated that, if he had found that the respondent was liable for authorisation, he would have held that the requirements of the safe harbour provisions were satisfied, with the consequence that the respondent would not have been exposed to all the remedies usually available for copyright infringement. The appellants say that his Honour was wrong to have found that the requirements of the safe harbour provisions were satisfied by the respondent.

FACTUAL BACKGROUND

541 The learned primary judge gave a lengthy and detailed account of the evidence. Very few of his Honour's findings of fact are challenged in the appeal. My summary of the relevant facts is drawn from the account provided by his Honour.

IP Addresses

542 The internet is a network of networks of computers. Protocols facilitate communication between computers over networks. The internet protocol (IP) enables data to be transmitted over networks in small packets containing headers which contain information identifying the IP addresses of the location from which the packet is transmitted and the location to which the packet is transmitted. These packets of data are not usually sent directly from one location to another due to the absence of direct connections between locations. They are instead transmitted via a series of locations before arriving at their ultimate destination.

543 An IP address is a binary number which, for convenience, may also be converted into a number consisting of four groups of three digits separated by a full stop. IP addresses are sold in blocks to ISPs who then allocate them to subscribers so that they may connect to the internet. In Australia, the body responsible for allocating IP addresses to ISPs is the Asia-

Pacific Network Information Centre (**APNIC**). The identity of the ISPs to whom particular IP addresses have been allocated is publicly available information.

544 Network address translation (**NAT**) allows a router (a device which can "route" data between a network of computers) to share one internet connection between a number of computers. Each computer connected to the router is assigned an IP address by the router in the same format as that used on the internet though in such a configuration the IP address for each of those computers is known only to computers on the network. But the IP address assigned to the router is public and can be seen by computers on different networks. NAT allows the number of computers connected to the internet to be dramatically increased because, with NAT, each computer does not need to have its own public IP address assigned to it in order to access the internet.

545 The location of a connection to the internet may be ascertained by means of the public IP address assigned to it by an ISP. However, if a number of computers are utilising a single connection via a router it will not be possible to identify which of those computers was connected to the internet at any particular time. To further complicate matters, most of the public IP addresses assigned by the respondent to its subscribers are dynamically assigned. This means that the public IP address assigned to a subscriber changes over time. These changes occur frequently, sometimes many times within an hour, though for the computer user this will at most result in a momentary reduction in speed of internet access.

546 ISPs generally keep records of public IP addresses assigned to particular accounts from time to time which allows them to know which public IP address is being used by a particular account. The account will generally be in the name of an individual or a company. Of course the ISP's records do not enable the ISP to identify the particular computer accessing the internet using a given IP address, much less the individual who uses that computer, who may or may not be the subscriber.

The BitTorrent protocol

547 The BitTorrent protocol (**BitTorrent**) is designed to facilitate the efficient distribution of data over the internet. It does this using a "peer to peer" system under which, in the primary judge's words, "all computers seeking data participate in the distribution of it" (at

[56]). The distribution of data is decentralised in the sense that a computer which is used to download a file utilising BitTorrent connects to a swarm of other computers also using BitTorrent and begins the process of downloading the file from, and uploading it to, other computers in the swarm. This is quite different to the traditional client/server model of data distribution under which one computer (the server) sends data to another computer (the client) which requests it. BitTorrent breaks up large files (which are often hundreds or thousands of megabytes in size) into smaller parts (pieces) which usually are somewhat larger in size than the packets in which they are transmitted.

548 A computer user wanting to download a file using BitTorrent must first install a BitTorrent client on his or her computer. This involves installing a computer program (**the BitTorrent client**) that enables the computer to receive and transmit data using BitTorrent. There are a number of different BitTorrent clients available free of charge from a variety of sources.

549 Once the BitTorrent client is installed, the computer user may then locate and download ".torrent files" which are available from many websites. These sites contain catalogues of torrent files associated with particular content, (for example, a movie or an episode of a television program). A torrent file contains the name of the file sought, the size of the file, the hash value of the file, the hash value of pieces of the file and the location of a "tracker".

550 When the computer user opens and runs a torrent file, the computer will communicate with other computers which run programs known as trackers. A tracker monitors a particular swarm associated with files containing particular content. Information obtained from the tracker, including the IP addresses used by computers in the swarm, is then utilised by the user's computer to download the pieces of the relevant content from peers in the swarm.

Peer ID

551 When a BitTorrent client is opened, it generates a "Peer ID" consisting of a random alphanumeric string which acts as an identifier of the BitTorrent client until the BitTorrent client is closed. When the BitTorrent client is re-opened a new Peer ID is generated. The Peer ID is visible to the rest of the swarm enabling others peers to identify the sources of the

pieces downloaded by them. A change in IP address does not trigger any change in the Peer ID. Where two or more pieces were downloaded by a BitTorrent client using the same Peer ID number, it can be inferred that those pieces emanated from the same computer regardless of any change in the IP address used by that computer.

AFACT

552 The Australian Federation Against Copyright Theft (**AFACT**) is an organisation associated with the Motion Picture Association (**MPA**) and the Motion Picture Association of America (**MPAA**) though, according to the primary judge, not by reason of any formal written agreement. His Honour described AFACT's relationship to the appellants as a "loose arrangement" involving the provision of services.

AFACT Notices to iiNet

553 On 2 July 2008 Mr Gane, as the Director of Operations of AFACT, and later Executive Director of AFACT, sent to the respondent the first of what were many letters (**the AFACT notices**) entitled "Notice of Infringement of Copyright". The letter was addressed to Mr Malone, the managing director of the respondent. Relevantly, the letter stated:

> 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…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.

554 Attached to the letter was a spreadsheet which was alleged to show that individual subscribers of the respondent, referred to in the AFACT Notice as "repeat infringers", were involved in multiple infringements of copyright. In addition to the information referred to by Mr Gane in the letter, the spreadsheets also included a column headed "% of File Shared". The vast majority of entries in the spreadsheet show this as 100%.

555 The letter also 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.

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.

556 Also attached to the letter was an extract from the respondent's Customer Relationship Agreement (**CRA**) pursuant to which the respondent provided internet services to its subscribers and an extract from a notice appearing on the respondent's website concerning copyright and illegal content. These extracts were as follows:

1. Customer Relationship Agreement (CRA):

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 directions 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, then 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.*

557 On 9 July 2008 a second AFACT notice was sent to the respondent which was in relevantly identical terms to the first except that it related to the period from 30 June 2008 to 6 July 2008. On 16 July 2008 a third AFACT notice was sent to the respondent which enclosed three DVDs. The DVDs incorporated the same information contained in the CDs that accompanied the earlier notices but also included additional information said to be the underlying data collected over the course of the investigations referred to in all three notices.

558 Thereafter, AFACT notices in similar terms were sent to the respondent every week until August 2009. By that time, the respondent had received AFACT notices recording allegations of copyright infringement against iiNet users and the data relating to those allegations for the period from 23 June 2008 to 9 August 2009.

iiNet's response to AFACT Notices

559 The AFACT notices of 2, 9 and 16 July 2008 were responded to by Mr Leroy Parkinson, the credit officer of the respondent. Mr Parkinson's letters are referred to briefly by the primary judge. In the first of them Mr Parkinson states that the respondent was very concerned about the allegations made in the AFACT notices. He suggested that AFACT direct its allegations to the appropriate authorities and provided the contact details of a police officer attached to the Computer Crime Squad of the West Australian Police. He referred to the expression "identified iiNet Customers" as used in the AFACT notices and made the point that the IP addresses referred to in them were not synonymous with particular people or entities. He also referred to the data provided by AFACT in support of its allegations and stated:

> … you have provided data containing IP addresses, dates, time and other details which are not explained, and some of which iiNet does not recognize.

560 The letter does not identify the "other details" referred to by Mr Parkinson nor any of the details which iiNet claimed not to recognise and, since he was not called as a witness, there was no direct evidence from him concerning those matters. The primary judge found that although the e-mails were written by Mr Parkinson, it was Mr Dalby, the chief regulatory officer of the respondent, who had oversight and responsibility for responding to AFACT.

Mr Dalby gave evidence that there were aspects of the AFACT notices that he did not understand at the time. The primary judge said he accepted (at [206]) that "… it is entirely possible that Mr Dalby did not understand the technical language used in the spreadsheet …" and (at [211]) that he was:

> … 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.

This is a reference to a letter sent by Mr Parkinson to Mr Gane on 12 August 2008. In it the respondent declined to take any action on the AFACT notices on the basis that it was not the responsibility of iiNet to act as "a law enforcement agency". As the primary judge found (at [207]) this letter suggested that the respondent would not be acting on AFACT notices even if it did understand them and that (at [208]) by the time the third AFACT notice was received (which included the additional data previously referred to) it was the respondent's position that it was not its responsibility to interpret the information supplied by AFACT.

561 It is also apparent from various other findings made by the primary judge that the respondent adopted a practice of not acting on notices sent to the respondent by or on behalf of copyright owners who alleged that their works or other subject-matter was being infringed by iiNet users. Most of these findings were made by the primary judge in relation to what was referred to as "the Westnet issue".

The Westnet issue

562 Westnet was another ISP which was acquired by the respondent in May 2008. It apparently received notices purportedly sent on behalf of copyright owners alleging that Westnet's users were infringing copyright. Westnet had a practice of forwarding copies of such notices to its subscribers. The primary judge accepted that there were no notices issued by AFACT to Westnet and that the notices it received were different from the AFACT notices in important respects. In particular, these notices were "robot" notices sent to Westnet by email. While his Honour was satisfied that the Westnet policy was in place as at September 2008 he said that he could not say how long it had been followed before then.

563 Mr Malone first became aware of the Westnet policy sometime in September 2008 but it was terminated by him shortly afterwards. The primary judge accepted Mr Malone's evidence that he thought the Westnet policy "damaging because the 'industry was in negotiation 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" (at [143]).

DtecNet Agent

564 The data provided to the respondent under cover of the AFACT notices was the primary evidence relied upon by the appellant to show that iiNet users had infringed copyright. It was collected by a company called DtecNet Software APS using proprietary software developed by it called "DtecNet Agent". The primary judge accepted that this evidence was reliable.

565 The DtecNet Agent acted in essence as a BitTorrent client but with additional functionality that enabled it to determine the identity of the public IP addresses and the Peer IDs of computers used to make available online or electronically transmit the appellants' films.

566 Using the appropriate .torrent file, the DtecNet Agent was able to connect to a tracker in the same way as any other BitTorrent client. The tracker would then provide the DtecNet Agent with the information necessary to enable it to connect to a swarm and download pieces of one of the appellants' films. The DtecNet Agent used an IP address filter which was configured to ensure that it only connected to iiNet users. Initially, the DtecNet Agent downloaded a complete copy of the relevant film. Steps were then taken by DtecNet staff to ensure that what was downloaded was an actual copy of one of the appellants' films.

567 The DtecNet Agent subsequently reconnected to the iiNet users' computers which were sharing the film and downloaded pieces from those computers. It then matched the downloaded pieces against the pieces originally downloaded to ensure that they were pieces of the same film. It repeated this process every 24 hours over a period of nine months or more. The records of these downloads show the period of time over which a particular film was made available online by a computer connected to the internet using public IP addresses

assigned by iiNet to its account holders. These records also include details of the Peer IDs generated by the BitTorrent clients that transmitted the pieces. Where the Peer ID was common to one or more of the transmitted pieces, it could be inferred that the same computer was responsible for transmitting all of those pieces.

568 The primary judge noted (at [272]) that the respondent admitted that where the DtecNet evidence showed a particular film as shared then that film had been made available online by an iiNet user even if the percentage shared was shown as something less than 100%.

The RC-20 Accounts

569 During the pre-trial discovery process the appellants provided the respondent with 45 IP addresses and times identified by DtecNet and the AFACT investigators, Mr Herps and Mr Fraser, as having infringed the appellants' copyright. The respondent was then able to match these IP addresses and times with its own records to identify 20 unique subscriber accounts. These became known as the "RC-20 Accounts".

570 The respondent then provided the appellants with information relating to those accounts for a period of time commencing from the date of the first AFACT notice. This information included login/logout details, allocation of IP addresses, time spent online as well as the reasons for disconnection. This data was then analysed and collated by the appellants to produce spreadsheets of the infringements alleged to have occurred in relation to each of the RC-20 Accounts. The primary judge described the RC-20 Accounts as "the most specific evidence of copyright infringement by iiNet users in these proceedings" (at [124]).

iiNet's repeat infringer policy

571 A considerable amount of time was taken up at the trial on the topic of the respondent's repeat infringer policy. In short, the appellants argued that the respondent did not have a repeat infringer policy. The primary judge rejected the appellants' argument and held that the respondent had such a policy (at [611]). His Honour also went on to hold that the respondent had adopted and reasonably implemented that policy.

572 The primary judge does not specify the terms of the respondent's repeat infringer policy except by reference to two documents that were in evidence and oral evidence given by Mr Malone.

573 The first document was an extract from a page on the respondent's website that stated:

> 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.

574 The second document is the CRA which enables the respondent to terminate subscriber accounts due to copyright infringement. The oral evidence of Mr Malone referred to by the primary judge (at [614]) made clear, according to his Honour, that the detail of the policy did not exist other than in Mr Malone's mind. As to what the detail of the policy was, the primary judge appears to have accepted Mr Malone's oral evidence to the effect that the termination of subscriber accounts would occur in three situations:

- when the respondent was ordered by a court to terminate a subscriber's account;
- when an iiNet user admitted to infringing copyright;
- when an iiNet user was found by a court or other authority to have infringed copyright.

COPYRIGHT ACT 1968

Part IV

575 For the purposes of this appeal, relevant provisions of the Act are found in Part IV (ss 84-113C) which is concerned with "Copyright in subject-matter other than works". This

includes cinematograph films and sound recordings as well as television and sound broadcasts.

576 Section 86 of the Act specifies the exclusive rights of the owner of copyright in a cinematograph film. It provides:

> 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) to cause the film, in so far as it consists of visual images, to be seen in public, or, in so far as it consists of sounds, to be heard in public;
>
> (c) to communicate the film to the public.

577 Section 101 relates to authorisation of acts comprised in the copyright of subject-matter other than works. Relevantly, s 101 provides:

> (1) Subject to this Act, a copyright subsisting by virtue of this Part is infringed by a person 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.
>
> (1A) In determining, for the purposes of subsection (1), whether or not a person has authorised the doing in Australia of any act comprised in a copyright subsisting by virtue of this Part without the licence of the owner of the copyright, the matters that must be taken into account include the following:
>
> (a) the extent (if any) of the person's power to prevent the doing of the act concerned;
>
> (b) the nature of any relationship existing between the person and the person who did the act concerned;
>
> (c) whether the person 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.

578 Section 112E provides:

> 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.

Part II

579 Other provisions relevant to the interpretation of the above provisions are contained in Part II (ss 10-30A) of the Act. Definitions of "communicate" and "to the public" are contained in s 10 of the Act. The latter is defined to mean "to the public within or outside Australia". The word "communicate" is relevantly defined to mean:

> … make available online or electronically transmit (whether over a path, or a combination of paths, provided by a material substance or otherwise) a work or other subject-matter …

580 Section 13 relevantly provides:

> (1) A reference in this Act to an act comprised in the copyright in a work or other subject-matter shall be read as a reference to any act that, under this Act, the owner of the copyright has the exclusive right to do.
>
> (2) For the purposes of this Act, the exclusive right to do an act in relation to a work, an adaptation of a work or any other subject-matter includes the exclusive right to authorize a person to do that act in relation to that work, adaptation or other subject-matter.

581 Section 14(1)(a) also provides that, unless the contrary intention appears, 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.

582 Section 22(6)-(6A) provides:

> (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.

Part V, Division 2AA

583 The safe harbour provisions, to which reference has already been made, are contained in Part V, Division 2AA of the Act.

584 Section 116AA specifies the purpose of Division 2AA. It 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.

585 Sections 116AC-116AF are in subdivision D. They define four different categories of activity. Section 116AC defines Category A activity as follows:

> A carriage service provider carries out a ***Category A activity*** by providing 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 provision of connections.

586 Section 116AG(1)-(3) provides:

> (1) A carriage service provider must satisfy the relevant conditions set out in Subdivision D before the limitations in this section apply.
>
> (2) For infringements of copyright that occur in the course of carrying out any of the categories of activities set out in Subdivision B, a court must not grant relief against a carriage service provider that consists of:
>
> (a) damages or an account of profits; or
>
> (b) additional damages; or
>
> (c) other monetary relief.
>
> (3) For an infringement of copyright that occurs in the course of the carrying out of a Category A activity, the relief that a court may grant against a carriage service provider is limited to one or more of the following orders:
>
> (a) an order requiring the carriage service provider to take reasonable steps to disable access to an online location outside Australia;
>
> (b) an order requiring the carriage service provider to terminate a specified account.

587 Section 116AH is also found in subdivision D. Section 116AH(1) includes a table that sets out the conditions for each of the categories of activity set out in ss 116AC-116AF. The parts most relevant for the purposes of the appeal are items 1 and 2 which are as follows:

Item	Activity	Conditions

Item	Activity	Conditions
1	All categories	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. 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.
2	Category A	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.

THE PRIMARY JUDGE'S REASONING

Primary Infringement

588 The primary judge recognised the importance of identifying the particular acts of infringement which the respondent was alleged to have authorised: see *WEA International Inc v Hanimex Corporation Ltd* (1987) 17 FCR 274 at 287-288 (Gummow J). His Honour also noted that acts of copyright infringement are necessarily acts of one or more persons. A computer can be used to commit an infringement of copyright but the act of infringement must be that of the person who uses the computer in an infringing way.

589 The primary judge found that iiNet users had infringed copyright by making copies of the films. It is apparent from his Honour's reasons as a whole that this finding related to the making of copies stored on the hard drives of computers of iiNet users who made these films available online. The primary judge also said that he was not prepared to find that iiNet users made copies of the appellants' films "on physical media (such as a DVD) for viewing purposes" (at [349]). It is apparent that the latter observation relates to physical media besides computer hard drives.

590 The respondent did not challenge the primary judge's finding that iiNet users had made copies of the films on the hard drives of the computers used to make such films available online. Nor did the appellants challenge his Honour's decision in so far as it related

to other physical media. But these are not the acts of primary infringement upon which the authorisation case hinges. The appeal has been conducted on the basis that the appellants can only succeed against the respondent if they establish that the iiNet users' infringements of the communication right were authorised by the respondent. It is necessary, therefore, to focus on the reasoning of the primary judge underlying the findings made by him in relation to the iiNet user's infringement of that particular right by iiNet users.

Make available online

591 The appellants argued before the primary judge that an iiNet user committed a new act of infringement of the appellants' copyright each and every time a computer on which one of the identified films was stored was connected to the internet and the film was made available online.

592 The primary judge rejected the appellants' argument on the ground that to construe the expression "make available online" in this way "would produce an entirely arbitrary and random result, in respect of the number of copyright infringements" (at [292]).

593 When addressing this issue the primary judge observed that a computer using IP addresses which were dynamically assigned may be disconnected and reconnected to the internet many times during a relatively short period of time. Thus, if the appellants' argument was accepted it would give rise to the possibility that a person whose internet connection was maintained using dynamically assigned IP addresses would be found to have engaged in many more acts of infringement when compared to another person whose internet access was provided by means of a static IP address, all other things being equal.

594 His Honour said that it was appropriate to focus on the substantive acts of the user rather than the technical process by which a file is made available online when considering how many times copyright in a film is infringed. His Honour explained (at [288]):

> … 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.

595 The primary judge also observed, referring no doubt to the definition of communicate in s 10, that "[t]he 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" (at [294]). In support of this observation his Honour referred to s 135ZWA(2A) of the Act as an example of a provision of the Act that took a temporal approach to making available online.

Electronically transmit

596 The respondent accepted before the primary judge that the films had been communicated by electronic transmission though it argued that they were not communicated by iiNet users to the DtecNet Agent but by the DtecNet Agent to iiNet users. If that is correct, the iiNet users could not be liable for infringement since they had not electronically transmitted the films. The respondent also argued that if iiNet users did electronically transmit the films then it was not established on the evidence that such transmissions were of a substantial part of the films or that such transmissions were to the public. In addressing these arguments, the primary judge referred to what he described as "significant hurdles" which stood in the way of a finding that iiNet users had infringed copyright in the appellants' films by electronic transmissions made using BitTorrent.

597 The first of the hurdles referred to by the primary judge centres upon the requirement of substantiality. As his Honour recognised, a person infringes the communication right if he or she makes an electronic transmission of the whole or a substantial part of a work or other subject-matter. Where less than the whole of a work or other subject-matter has been electronically transmitted by a person alleged to have infringed copyright, it is necessary to determine whether the part transmitted constitutes a substantial part of the whole. In this context, his Honour said (at [304]):

> … 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 …

598 His Honour went on to say that by adopting what he described as the "correct approach", it was unnecessary for him to undertake any such analysis. This involved taking a "broad approach" under which the relevant electronic transmission was that sent by the iiNet user to all other BitTorrent clients (including the DtecNet Agent) making up a swarm. His Honour stated (at [310]-[312]):

> 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.
>
> 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.
>
> 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.

599 The second of the hurdles referred to by the primary judge centred upon the requirement that there be a communication to the public. His Honour referred to a submission made by the respondent to the effect that an electronic transmission must be made to the public before it could be found to be infringing and that this raised the question of whether the electronic transmission of pieces between peers in a swarm occurred in a "commercial context": see *Telstra Corporation Ltd v Australasian Performing Right Association Ltd* (1997) 191 CLR 140 at 157. The primary judge again took the view that it was unnecessary for him to deal with that submission (at [309]).

600 The third of the hurdles referred to by the primary judge was the fact that an iiNet user would only be liable for infringing copyright in the appellants' films if that iiNet user made the electronic transmission. After referring to s 22(6) and s 22(6A) of the Act his Honour stated that there was a disagreement between the parties at a technical level as to how "each communication of a piece of the file between peers is effected by the BitTorrent protocol" (at [323]). His Honour then stated (at [324]-[325]):

> 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.
>
> 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.

601 It is also necessary to refer to the primary judge's finding that "each iiNet user 'electronically transmits' each film once." His Honour said (at [316]-[317]):

> 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.
>
> 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*.

Authorisation

602 The primary judge began his analysis of the issue of authorisation with a detailed examination of the judgments of Gibbs J and Jacobs J (with whom McTiernan J agreed) in *University of New South Wales v Moorhouse* (1975) 133 CLR 1. His Honour referred to statements in both judgments that "authorise" had previously been held to mean "sanction, approve, countenance" (*Falcon v Famous Players Film Co* [1926] 2 KB 474 at 491) and Gibbs J's statement to the effect that while "authorise" had been held to mean "permit", a person could not be said to have authorised an infringement unless he or she had some power to prevent it (*Adelaide Corporation v Australasian Performing Right Association Ltd* (1928) 40 CLR 481 at 497-498, 503).

603 The primary judge (at [369]) placed considerable reliance upon a passage which appears in the judgment of Gibbs J (at 133 CLR at 13) which refers to "the means by which an infringement may be committed". I will refer to that passage in greater detail later in these reasons since it is central to his Honour's analysis. For present purposes it is sufficient to say that the primary judge reasoned, relying upon that passage, that the first consideration in

Moorhouse was whether the university (the defendant which had made the photocopying machine and library books available to students) had provided the "means" by which an infringement may be committed. This represented the beginning of the core approach taken by the primary judge to the issue of authorisation which involved asking, first, what were the "means" with which the primary infringements were committed and, secondly, whether the means of infringement were provided by the respondent to the iiNet users who had infringed the appellants' copyright.

604 The primary judge then drew the following conclusions on the basis of the judgment of Gibbs J and Jacobs J in *Moorhouse* (at [381]-[382]):

> 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 …
>
> 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 ... 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.

605 His Honour went on to hold that the respondent did not provide the means by which iiNet users committed infringements of the appellants' copyright. He found that BitTorrent was the means by which the appellants' copyright was infringed and, as was common ground, that it was not provided to iiNet users by the respondent.

606 Later in his reasons (at [414]) the primary judge restated his principal conclusion to the effect that the respondent could not be taken to have authorised iiNet user's infringement because it did not provide them with the means of infringement. It was only at this point in the primary judge's reasons that he appears to have turned to the specific requirements of s 101(1A) of the Act.

Section 101(1A)(a) – power to prevent

607 The primary judge noted (at [418]) that it was common ground between the parties that control must be found to exist before there can be a finding of authorisation. He then

referred to *Cooper v Universal Music Australia Pty Ltd* (2006) 156 FCR 380 (at [41]) and set out the following statement appearing in the judgment of Branson J:

> 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.

608 His Honour criticised this statement, implicitly at least, suggesting that it was not consistent with the High Court finding in *Australian Tape Manufacturers Association Ltd v Commonwealth* (1993) 176 CLR 480 that a vendor of tapes or tape records had no relevant control over them after their sale. The primary judge also referred to the reasons of Higgins J in *Adelaide Corporation* (at CLR 498-499) which suggest that notions of reasonableness and the power to prevent infringement interact. The primary judge found that the same interaction occurred between sub-par (a) and (c) of s 101(1A) of the Act.

609 His Honour said that in other cases apart from *Adelaide Corporation* "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" (at [422]).

610 After referring to his earlier findings concerning "means of infringement", his Honour said (at [424]) "… 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." I take his Honour to mean by this that this was the only power that could arguably qualify for consideration for the purposes of s 101(1A)(a). His Honour referred to other steps that the appellants suggested at trial might be taken by the respondent but rejected these due to what he described as a "lack of evidence".

611 Thus, his Honour found that the respondent had power to prevent infringement by warning, suspension and termination. However, his Honour went on to conclude that this was not a relevant power because the respondent could not reasonably be expected to exercise it for the purpose of preventing copyright infringement by iiNet users. In the course of arriving at this conclusion his Honour rejected the four main grounds upon which the appellants relied in support of their submissions to the contrary.

612 First, the appellants relied upon the CRA which they said gave the respondent the ability to suspend or terminate accounts. The primary judge appears to have accepted that the CRA did so but said (at [427]) that without the benefit of any indemnity from the appellants or AFACT "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".

613 Secondly, the appellants drew attention to the fact that the respondent suspends or terminates its subscribers from time to time for non-payment. His Honour did not consider this comparable to suspension or termination for copyright infringement. The former was straightforward and attended by a far greater degree of certainty. Copyright infringement, his Honour said, was not a straightforward question.

614 Thirdly, the appellants argued that the safe harbour provisions expressly envisaged the termination of subscriber accounts and that it therefore should be considered a reasonable step for the respondent to take. His Honour rejected this argument on the basis that it was circular and that it reflected a misunderstanding of the safe harbour provisions. He said (at [431]) that the "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." His Honour also referred to the relevant words used in the safe harbour provisions and commented upon their lack of definition.

615 Fourthly, the appellants relied upon the fact that the respondent had the technical capability to suspend and terminate accounts. His Honour accepted that the respondent had that capability but said that the question of whether or not it should be exercised in any particular case was a complex one.

616 His Honour also found (at [433]) that a policy like that followed by Westnet, which involved passing on infringement notices to subscribers, "… 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 …". He said that "an ineffectual step is not a power to prevent infringement nor is it a reasonable step".

617 There were other reasons given by the primary judge for rejecting the appellants' submissions on this issue. These focused upon what his Honour considered to be the difficulty for the respondent in knowing how many warnings should be issued prior to termination and the extent to which reliance could be placed upon notifications of various kinds. The primary judge also referred (at [437]) to the RC-20 accounts as containing what would appear to be some of the worst examples of iiNet users who were proven to have infringed copyright. His Honour said that the extent to which those accounts were used for the infringement of the appellants' copyright was not clear from the evidence.

618 His Honour concluded his consideration of s 101(1A)(a) by finding (at [444]) that the respondent had no relevant power to prevent the infringements which were occurring. He added that this was "unfortunate" but that "the fault lies with the applicants for choosing the wrong respondent."

Section 101(1A)(b) – the nature of any relationship

619 The primary judge accepted that there was a contractual relationship between the respondent and its subscribers governed by the provisions of the CRA but said he did not consider this sufficient to justify any different finding on the issue of authorisation to that previously made by him.

Section 101(1A)(c) – other reasonable steps

620 The primary judge referred to the judgment of Gibbs J in *Moorhouse* (at 133 CLR 14) and said that the taking of reasonable steps to prevent infringement operates as "somewhat of a defence or exculpation to authorisation" and that, under more recent authority, a failure to take such step could be evidence of authorisation.

621 On the question whether the respondent took any reasonable steps to prevent or avoid copyright infringement by iiNet users, his Honour referred (at [459]) to evidence concerning the RC-20 accounts which showed that the respondent had the ability to restrict a subscriber's internet access to the respondent's website only where the subscriber's account was suspended for non-payment. However, his Honour said there was "insufficient evidence to prove that it would be technically possible for the respondent to implement such block on all subscriber accounts" (at [459]). His Honour also referred to the blocking of access to specific

websites. Here again, the evidence was, according to his Honour, insufficient to prove that it would have been feasible for the respondent to block its users from accessing particular websites. His Honour also noted (at [460]) that this was not a step which the AFACT notices suggested the respondent should take.

622 While the primary judge does not mention the use of warning notices in his consideration of s 101(1A)(c), it is clear from what his Honour had earlier said (at [433]) that, in his view, passing on warning notices could not, without more, be considered a reasonable step because warning notices would be ineffectual if not followed up by termination.

Section 101(1A) – other considerations

623 The primary judge recognised that it was open to him to take other considerations into account when considering whether or not a person had authorised an infringing act beyond those expressly identified in s 101(1A). The additional considerations referred to by his Honour were "knowledge of infringement", "encouragement of infringement" and "inactivity or indifference" to infringement.

KNOWLEDGE OF INFRINGEMENT

624 The primary judge accepted that knowledge that copyright infringement was occurring was a relevant matter. His Honour noted that the respondent accepted that it had a general knowledge that iiNet users were using its facilities to infringe but found that at that level of abstraction it would be very difficult for the respondent to act on such knowledge in any meaningful way.

625 The primary judge then turned to the AFACT notices. His Honour found (at [430]):

> 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.

His Honour also found that ISPs (including the respondent) had, both before and after the AFACT notices were served, also received thousands of robot notices generated overseas from data which his Honour said had been shown to be unreliable. His Honour said at [468] that in those circumstances, "there was an obligation on AFACT to make clear that their data

was different if they expected a positive response" and that AFACT should have explained in detail how the DtecNet Agent operated so that the respondent could understand how the copyright allegations came to be made. His Honour found that no such explanation was given to the respondent until after the proceeding was commenced. Only then, on his Honour's findings, did the respondent possess the knowledge which enabled it to act.

ENCOURAGEMENT OF INFRINGEMENT

626 The primary judge observed that failing to stop infringing conduct occurring was not the same as encouraging infringing conduct. He then referred to a press release and radio advertisement published by the respondent which were relied upon by the appellants in support of a submission that the respondent had encouraged iiNet users to infringe copyright. The appellants also submitted that by encouraging iiNet subscribers to use more bandwidth or quota the respondent was encouraging copyright infringement. Both submissions were rejected by the primary judge on the basis that none of the conduct relied upon by the appellants amounted to encouragement to infringe copyright.

"INACTIVITY OR INDIFFERENCE"

627 The appellants submitted to the primary judge that the respondent's failure to act on the AFACT notices was evidence of inactivity or indifference toward iiNet users' infringement of copyright in the appellants' films from which authorisation could be inferred: see *Moorhouse* at 133 CLR 12 per Gibbs J. His Honour rejected this submission on the basis that it made no allowance for the fact that the respondent did not provide its subscribers with the means of infringement and that it therefore had no relevant power to prevent infringements occurring. His Honour considered "indifference" to be irrelevant in such circumstances.

"sanction, approve, countenance"

628 The primary judge then came to consider when determining whether the respondent had authorised iiNet users' copyright infringements the question whether the respondent could be said to have "sanctioned, approved, countenanced" the iiNet users' infringements. His Honour said that these terms had to be read conjunctively. His Honour also said that they implied "a sense of official approval or favour of the infringements which occur" and that no

such approval or favour could be found on the facts of the present case. In support of that conclusion the primary judge referred to, amongst other things, various public statements made by Mr Malone in late 2008 and early 2009 to the effect that the respondent did not support or encourage breaches of the law, including the infringement of copyright. His Honour rejected any suggestion that the respondent tacitly approved of copyright infringement and found that the respondent did not intend, and had never intended, that its facilities be used to infringe.

Telco Act

629 The primary judge considered the provisions of the Telco Act relevant to the respondent's submission that it could not act on the AFACT notices by warning, suspending or terminating its subscribers for copyright infringement. I have had the advantage of reading the reasons for judgment of Jagot J. I gratefully adopt her Honour's summary of the primary judge's findings on this issue and the arguments relied upon in the appeal.

Section 112E

630 The primary judge referred to the legislative history of s 112E and previous authorities concerning its meaning and effect. His Honour interpreted those authorities as establishing that for conduct on the part of a person to constitute authorisation he or she must do more than merely provide facilities for making or facilitating the making of a communication and it therefore followed that there was little room for s 112E to have any meaningful operation.

631 The primary judge concluded that the respondent would not have avoided a finding of authorisation by virtue of s 112E because it could never have satisfied the requirements of the section. On his Honour's reasoning, the respondent had, at some point at least, knowledge of infringements sufficient to enable it to act on them and on the authorities referred to by him, that finding was in itself sufficient to place the respondent outside the operation of s 112E.

Safe harbour provisions

632 Earlier in these reasons, I referred to his Honour's finding that the respondent had a "repeat infringer policy". That policy, which provided for termination of subscriber accounts

in three different situations, was found by his Honour to be "a policy that provides for the termination, in appropriate circumstances, of the accounts of repeat infringers" for the purposes of the safe harbour provisions. His Honour referred to the legislative history of the safe harbour provisions and ancillary regulations and drew attention to what he described as the complete vacuum of legislative guidance in relation to this particular condition.

633 His Honour noted that the safe harbour provisions were modelled on very similar provisions in force in the United States. He considered a number of the authorities in which those provisions were considered but rejected the submission made by the appellants on the strength of them that a service provider must do what it can reasonably be asked to so to prevent the use of its service by repeat infringers. His Honour said that the requirements of any repeat infringer policy appear to be minimal, allowing service providers significant latitude to determine the policy.

634 In relation to policy implementation, his Honour said (relying on US authority) that a service provider was not allowed to take positive steps that had the effect of preventing a copyright owner from being able to give notice of alleged infringing activity. Significantly, the primary judge (also relying on US authority) said that (at [609]):

> … 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*' …
>
> [Emphasis added]

635 His Honour also found that the respondent's repeat infringer policy had been reasonably implemented in circumstances where up to that time no iiNet user had been found by a court to have infringed copyright and the respondent had not been ordered by a court to terminate any account. His Honour accepted that the respondent's policy set a high bar but said that, in the case of Category A activities, this was appropriate. In the result, his Honour held that the respondent had satisfied the requirements of the safe harbour provisions applicable to that category of activity.

THE GROUNDS OF APPEAL

636 The first ground of appeal raised by the appellants concerns the primary judge's approach to the issue of authorisation. The appellants say that this was wrong in the following respects:

(i) in determining the question of authorisation either wholly or substantially by reference to the question of who provided the "means of infringement".

(ii) in determining authorisation by reference to the concept of "means of infringement" separately from, and before, considering the matters he was obliged to consider under s 101(1A) of the Act for the purposes of determining whether there was authorisation.

(iii) in holding that an absolute "power to prevent" the doing of an act, or a contractual or technical capacity to prevent the doing of an act, do not separately or together constitute a power to prevent, or a "relevant" power to prevent, for the purposes of s 101(1A)(a) of the Act.

(iv) in holding that a person does not have the power to prevent the doing of an act for the purposes of s 101(1A)(a) of the Act if the exercise of that power is not a reasonable step for the purposes of s 101(1A)(c) of the Act.

(v) in holding that unless a party could prevent infringements without also preventing persons from undertaking non-infringing activities, the exercise by that party of such a power could not amount to a reasonable step for the purposes of s 101(1A)(c) of the Act.

(vi) in proceeding on the basis that it was for the applicants to identify precisely a step or series of steps which, if taken by the respondent, would constitute reasonable steps for the purposes of s 101(1A)(c) of the Act sufficient to avoid a finding of authorisation.

(vii) in holding that in order to find authorisation it was necessary to find that a person sanctioned, approved and countenanced infringements and that there be a "sense of official approval" or "favour" of infringements.

(viii) in holding that authorisation cannot be implied from indifference or inactivity in the face of knowledge of copyright infringement, even where a party has control or a power to prevent infringements.

637 There are a number of preliminary points that should be made about certain aspects of the first ground of appeal.

638 First, para (vi) of the first ground of appeal refers to the need for the applicants (the appellants) to "identify precisely a step or series of steps" that the respondent might reasonably have taken to prevent or avoid infringement. What is meant by "precisely" in this context is not altogether clear. However, I do not think it can be doubted that it was for the appellants to establish that there were "reasonable steps" that the respondent might have

taken, but omitted to take, which, together with other things, might justify a finding that the respondent had authorised copyright infringement. To that end, it was necessary for the appellants to identify the omitted "reasonable steps" upon which they relied to justify a finding of authorisation. Indeed, that is what the appellants did when they provided particulars of "reasonable steps" for the purposes of s 101(1A)(c). I will return to those particulars later in these reasons.

639 Secondly, as to para (viii) of the first ground of appeal, I do not think the primary judge made any such holding. As a general proposition, what is said in para (viii) is not correct though, as I say, I do not think his Honour endorsed any such general proposition in any event. What his Honour did say was that indifference or inactivity was irrelevant where the party alleged to have authorised infringement had no relevant power to prevent the primary act of infringement. That raises a different issue to which I will return.

640 The appellants also rely upon the following factual errors which they say were made by the primary judge in considering the case of authorisation:

(i) in holding that the "BitTorrent system" constituted the "means" by which the applicants' copyright was infringed by users of the respondent's services.

(ii) in holding that although the internet access provided by the respondent, while a necessary precondition for infringement to occur, did not constitute or form part of the "means" of infringement.

(iii) in holding that the ability of the respondent to warn subscribers and to suspend or terminate subscriber accounts, whether taken separately or together, did not constitute a power to prevent, or a "relevant" power to prevent, for the purposes of s 101(1A)(a) of the Act.

(iv) in holding that the respondent's other technical mechanisms for restricting access to its internet services, such as play-penning (restricting accounts) and blocking websites, whether taken separately or together, did not constitute a power to prevent, or a "relevant" power to prevent, for the purposes of s 101(1A)(a) of the Act.

(v) in holding that it was not in the financial or commercial interests of the respondent for users of its services to engage in infringement and that there was "no sufficient nexus between profitability and the commercial interests of the respondent" in order for there to be a relationship for the purposes of s 101(1A)(b) of the Act.

(vi) in holding that none of the measures identified in paragraphs (iii) and (iv) above, if taken, would have been a reasonable step for the purposes of s 101(1A)(c) of the Act, "at least absent judicial consideration of the extent of the infringement on each account".

(vii) in holding that the AFACT notices did not constitute sufficient or adequate notification to the respondent that iiNet users were infringing the applicants' copyright.

(viii) in finding that the respondent had not sanctioned, approved or countenanced the infringing acts of users of its services, or encouraged the doing of such acts, or been inactive or indifferent towards the doing of such acts.

641 The fifth of the asserted factual errors (referred to in para (v)) was not the subject of any submissions at the hearing of the appeal and was effectively abandoned by the appellants. In the result, there is no challenge to the primary judge's rejection of the appellants' assertion that the respondent profited from copyright infringement occurring over its network or that it was otherwise in the respondent's commercial interests to have its customers or network users engage in copyright infringement. I see that as significant because it cannot be inferred, given the primary judge's rejection of that part of the appellants' case, that any inactivity or indifference on the part of the respondent could be explained on the basis that it was in the respondent's financial interests that copyright infringement continue to occur.

642 So far as the issues of primary infringement are concerned, the appellants say that the primary judge also erred in:

(i) holding that a user made each film available online only once through the "BitTorrent system" (at [288]) and that a user electronically transmitted each film only once through the "BitTorrent system".

(ii) failing to find that copyright was infringed each time a computer on which the relevant file was located was connected to the internet.

(iii) holding that an electronic transmission in BitTorrent is not "a series of single acts" but is a "single ongoing process" of communication.

643 The appellants also say the primary judge should have concluded that there were numerous and repeated acts of infringement by users of iiNet's internet services. In this regard, they complain of what the appellants say was his Honour's failure to act on his own findings and also, as a separate point, his Honour's treatment of the evidence of the AFACT investigators, Mr Herps and Mr Fraser. The appellants say that the primary judge was wrong not to rely upon that evidence.

644 The appellants say that the primary judge also erred in his approach to the safe harbour provisions. In particular the appellants say the primary judge erred in:

(i) holding that the adoption by a carriage service provider (**CSP**) of a repeat infringer policy of the kind required by condition 1 of item 1 of s 116AH(1) of the Act (**the safe harbour provision**) could constitute evidence relevant to the question whether the CSP had authorised copyright infringement, but that the failure by the CSP to adopt such a policy would be "wholly irrelevant" for that purpose.

(ii) holding that a policy of the kind required by the safe harbour provision could exist even though it does not provide clear steps leading to termination, and does not mention the phrase "repeat infringer".

(iii) when, having adopted the US authority on the interpretation of the equivalent provision s 512(i)(1)(A), in holding that it was not necessary for a CSP to have a policy of the kind required by the safe harbour provision to have a mechanism for notifications to be provided to it alleging copyright infringement.

(iv) holding that for the purpose of a policy of the kind required by the safe harbour provision it is necessary for a CSP to be able to independently verify the allegations made pursuant to the policy and that for Category A activity the policy must meet the same requirements as those for Categories B-D activities.

645 The appellants also say that the primary judge erred in holding that the respondent had adopted and reasonably implemented a "repeat infringer policy", the details of which did not exist except in the mind of Mr Malone and which only provided for termination in the three situations nominated by him.

646 It is important to mention that while the appellants' notice of appeal asserted that the primary judge erred in accepting the evidence of Mr Malone and Mr Dalby, this ground of appeal was expressly abandoned by the appellants. Consistent with this position, the appellants made no attempt during the course of the hearing of the appeal to show that evidence given by Mr Malone or Mr Dalby was "glaringly improbable" or that it was otherwise open to this Court to dismiss or discount it on some like basis: *Fox v Percy* (2003) 214 CLR 118 at [20]-[31].

THE NOTICE OF CONTENTION

647 The respondent's notice of contention covers four different areas. The first of these concerns the matter of primary infringement.

648 The respondent contends that the primary judge erred in finding that, for the purpose of determining whether the conduct of iiNet users infringed the exclusive right of the

appellants to "electronically transmit" a substantial part of a film to the public, the relevant act of electronic transmission occurs between the iiNet user/peer and the BitTorrent swarm, not between each individual peer.

649 The respondent also contends that the primary judge should have determined whether what it says is the relevant electronic transmission (ie. that occurring between individual peers) involved the transmission of a substantial part of the relevant film by an iiNet user to the public. It contends that none of the relevant electronic transmissions was made by an iiNet user, that none of them was made to the public, and that none has been established to involve a substantial part.

650 The second area covered by the respondent's notice of contention concerns s 112E of the Act. The respondent contends that the primary judge erred in finding that as iiNet had knowledge of infringements that were occurring on its facilities and as such factor is relevant to a finding of authorisation, s 112E of the Act ceased to have operation. The respondent contends that the Full Court decision in *Cooper* did not compel such a finding but, if it did, then it was wrongly decided and should not be followed.

651 The third area covered by the respondent's notice of contention concerns his Honour's interpretation of relevant provisions of the Telco Act which the respondent says was incorrect.

652 The fourth area covered by the respondent's notice of contention relates to the safe harbour provisions and his Honour's construction of the phrase "accounts of repeat infringers" in condition 1 of item 1 of s 116AH(1) of the Act. The respondent contends that the primary judge should have found that the adoption and reasonable implementation of a repeat infringer policy need only occur in relation to repeat infringers who were also account holders. The respondents rely upon this as providing an additional reason for holding that "appropriate circumstances" for the termination of any account had not yet arisen and that iiNet had adopted and reasonably implemented a repeat infringer policy.

CONSIDERATION

Nature of the proceeding

653 It is necessary to say something more concerning the nature of the proceeding heard and determined by the primary judge. The proceeding was commenced by application and statement of claim asserting that the respondent was liable for copyright infringement because it had authorised multiple infringements of the appellants' copyright committed by iiNet users since at least July 2008. That was, as I have already mentioned, the month in which the first AFACT notices were sent to the respondent. An amended application and further amended statement of claim were filed on 8 May 2009. Supplementary particulars to the further amended statement of claim were filed on 18 September 2009 which particularised further infringements for the period 13 March 2009 to 6 September 2009.

654 The proceeding was not, contrary to a submission made by the appellants during the hearing of the appeal, in the nature of a proceeding for quia timet relief. It was certainly not pleaded that way and Mr Cobden SC, who appeared for the respondent on the appeal and at the trial, stated that the case against the respondent was never argued that way at the trial. As pleaded and conducted before the primary judge, the appellants' case was that the respondent had engaged in copyright infringement by authorising the infringing acts of iiNet users. In my opinion, if the appellants are to succeed in their appeal, it is necessary for them to establish that the respondent had infringed copyright either by the time the proceeding was commenced or, at the latest, by the time of the 8 May 2009 amendments: see O 13, r 3A of the *Federal Court Rules* 1979 (Cth).

655 The point is significant because the question of when the respondent first became aware of the details of the methods used to acquire the information accompanying each of the AFACT notices is material to the questions concerning the nature and extent of the respondent's knowledge of primary infringements and the circumstances in which that knowledge was first acquired. As I will later explain, the respondent's knowledge of such matters was only acquired after the commencement of the proceeding, and then only through expert reports supplied on a confidential basis and, as might be expected, solely for the purposes of the proper conduct of the proceeding. Questions obviously arise as to whether information made available on such a basis can or should be used for the purpose of finding a respondent liable for authorising other people's acts of infringement where that liability

depends upon, amongst other things, the respondent's state of knowledge at a particular point of time. Regardless of how those questions are answered, I do not think it is open to the appellants to avoid the potential difficulties involved by recasting what was in substance and form a proceeding for relief in respect of past and continuing infringement as one in which quia timet relief was sought for infringements that had not yet occurred or, at least, had not occurred by the time the application and statement of claim were last amended.

Primary infringements

656 The owner of copyright in a cinematograph film enjoys the exclusive right to communicate the film, or any substantial part of it, to the public (s 86(c), s 14(1)(a)). For this purpose, "to the public" means "to the public within or outside Australia" (s 10). The phrase "to the public" has a particular meaning in this area of the law to which it will be necessary to return later in these reasons.

657 The exclusive right to communicate only extends to acts of communication done in Australia. This is made clear by s 101(1) of the Act which provides that copyright is infringed by a person who does in Australia, or authorises the doing in Australia, of an act comprised in the copyright.

658 It is necessary to identify the particular act the doing of which is alleged to infringe copyright not only to identify the alleged infringer but also to see whether that act was done in Australia. The fact that the phrase "to the public" is defined as it is does not mean that the act must not be done in Australia. It means that the act must be done in Australia to the public within or outside Australia.

659 Accordingly, for the purpose of determining whether the right arising under s 86(c) has been infringed, it is necessary, as a first step, to identify the person who is said to have made the relevant communication. It is at this stage that s 22(6) and s 22(6A) of the Act become relevant. If the communication was made by that person in Australia then the next step is to determine whether it was made to the public.

The definition of "communicate"

660 The definition of communicate in s 10 has two limbs each of which encompasses a different type of activity.

661 The first limb, which consists of making available online, covers a situation where a person makes a film available on the internet. How widely the film is made available is relevant only to the question of whether it is made available to the public. The act of communication by making available online does not require that there be any actual communication in the ordinary sense of that word. A person who uses a computer to make a film available online "communicates" it for the purpose of s 86(c) whether or not it is transmitted to or accessed by any other person.

662 In the case of the second limb of the definition, which uses the expression "to electronically transmit", there must be an electronic transmission of the film. But here again, the definition of communicate does not require that the electronic transmission be made to another person in the ordinary sense of that word. There is no requirement that the transmission be received by any person within or outside Australia. All that is required is that there be an electronic transmission.

663 It is the combined effect of s 101 and s 86(c) which requires that there be an electronic transmission made by a person in Australia to the public. The fact that the public for this purpose includes the public outside Australia makes it clear that the transmission need not begin and end in Australia. Further, while the act of communication must be done in Australia, it need not be done by a person who is physically in Australia. A person who is physically outside Australia who makes a film available online to the public in Australia, does the act referred to in s 86(c) in Australia. And if that person electronically transmits the film to the public in Australia from outside Australia he or she likewise does the act referred to in s 86(c) in Australia.

Did iiNet users commit multiple acts of infringement by making available online?

664 In the present case the respondent conceded that iiNet users had communicated the films by making them available online. It also conceded that the films were made available online to the public.

665 The only question of principle raised in relation to the first limb of the definition of communicate relates to the proper characterisation of the relevant act. On this point, the primary judge found that a person who uses a computer to make a film available online by connecting to the internet does so only once, irrespective of how often, for how long or for what reason that connection is interrupted. With great respect to the primary judge, I do not think this is correct.

666 The primary judge's answer to this question seems to me to ignore the very nature of the act referred to in the first limb of the definition. Copyright material is either available online or it is not. When it is stored on a computer that is configured by its user so as to be accessible to others by means of an internet or other online connection then it will no longer be accessible if the user later terminates the connection. At that point it will not be available online. When the user takes steps to restore the connection, the copyright material will once again be available online.

667 The construction of the definition preferred by the primary judge produces surprising results. It means that a person who infringed copyright by making copyright material available online who later ceased to do so in response to a complaint from a copyright owner or in compliance with an order would not commit a further act of infringement if he or she subsequently made the same copyright material available online. Yet that seems to be the logical consequence of the primary judge's interpretation of the definition.

668 However, I do not think it follows that copyright material ceases to be available online every time there is a brief interruption to the online connection. The findings of the primary judge make clear that interruptions that occur through the use of dynamically assigned IP addresses are fleeting with the only perceptible result being a slight reduction in network speed at most. I do not think it could be said of that situation that the copyright material was no longer available online. The fact that the connection is intermittently interrupted in this way during the very process of making the copyright material available does not mean that it is no longer available. It would be more accurate to say that the copyright material remains available online but that it is only accessible at a reduced speed.

669 As for other interruptions that may occur to the online connection, an issue may arise as to whether the interruption is sufficient in duration and effect to justify the conclusion that

copyright material is no longer available online. If a person makes copyright material available online using a computer configured for that purpose and the online connection is interrupted for reasons beyond his or her control then it may be correct to say (depending on the length and effect of the interruption) that the copyright material was no longer available online. But no matter how that issue is resolved, I think the conclusion that a person who makes copyright material available online using a computer which he or she configures, unconfigures and then reconfigures (by opening or closing a program or turning the computer on or off) with the result that copyright material is available or not available at various times will have made the copyright material available online more than once. All other things being proven, that person will have committed more than one act of infringement.

670 On any reasonable understanding of the evidence, the appellants established that there were iiNet users who configured, unconfigured and then reconfigured their computers in this way. The primary judge found that a new Peer ID was assigned to a BitTorrent client each time it was reopened. When the evidence is interpreted in the light of that finding, it is apparent that individual iiNet users made the appellants' films available online on multiple occasions.

671 The primary judge found that the user of account RC-08 made the film Pineapple Express available online between November 2008 and May 2009. However, Exhibit MJW-10, which contains a summary of data relating to this account, shows the relevant BitTorrent client was closed during most if not all of February 2009 and did not reopen (at least not for a period of 24 hours or more) until the next month. This evidence shows that the user of account RC-08 made the film Pineapple Express available on more than one occasion between November 2008 and May 2009.

672 Similar examples can be found in the evidence. The records for RC-44 shows that the film "Hancock" was available online between October 2008 and January 2009 and that the relevant BitTorrent client was closed and not reopened (at least not for a period of 24 hours or more) between 9 and 26 January 2009. The records for RC-12 show that the film "Wanted" was made available between August and September 2008 but that there was a period of approximately 2 weeks during this period in the latter half of August 2008 when the relevant BitTorrent client was closed (at least once) before being reopened again.

673 I therefore accept that the appellants (who were put to strict proof on this issue) established that various iiNet users made copies of the appellants' films (including the three that I have identified) available online on multiple occasions during 2008 and 2009. On the other hand, I also accept that the appellants' treatment of dynamically assigned IP addresses in the infringement analysis upon which it relied was likely to have vastly overstated the number of separate acts of infringement committed by those users.

Did iiNet users commit multiple acts of infringement by electronic transmission?

"ELECTRONICALLY TRANSMIT"

674 The process by which a person obtains a copy of a film using BitTorrent has already been described. With BitTorrent, each peer making up the swarm responds to a request for a particular film by transmitting pieces to the requesting BitTorrent client which are then used by it to make a complete copy of the film. How many pieces are transmitted by a peer varies but for present purposes I shall assume that the figure is at least one.

675 There are therefore two relevant electronic transmissions being made when a person uses BitTorrent to download a copy of a film. The first is the electronic transmission of pieces from the peers (or a "swarm" of peers) to the client which I have already discussed. The second is the electronic transmission of pieces from the client to the peers. When the client begins receiving pieces it will also start to transmit at least some of the pieces it has acquired to other clients seeking to download the film.

ELECTRONIC TRANSMISSION FROM SWARM TO CLIENT

676 The first question that arises is whether there is an electronic transmission of a copy of the film or a substantial part of the film by the swarm to the client. The primary judge's analysis of this issue treated the various transmissions sent to the client by the peers that make up the swarm as one transmission. His Honour found, in effect, that there was in substance one transmission of the whole of the film rather than a series of different transmissions consisting of many tiny fragments of the whole film.

677 The words "electronically transmit" in the definition of "communicate" do not require that there be a single electronic transmission. Where a person uses the internet to transmit a

film the question whether the film has been communicated by him or her cannot depend on whether the film is transmitted in one or more separate transmissions or one or more separate files. If the film is too large to be conveniently transmitted in one file then it will usually be broken down into smaller files each of which may be transmitted in rapid succession. But whether the files are transferred in rapid succession or whether they are instead transferred over a period of minutes or hours is immaterial. The whole film will have been electronically transmitted for the purposes of the definition. Similarly, the fact that BitTorrent transmits a film in the form of many tiny pieces does not mean that the whole (or a substantial part) of the film is not electronically transmitted.

678 Nor do the words of the definition require that the electronic transmission occur over a single path. They expressly contemplate the possibility that the electronic transmission may occur over a combination of paths. If a person transmitted the different pieces which make up the whole film over a combination of paths he or she will have still transmitted the whole film.

679 In the respondent's analysis of the process by which a person obtains a copy of a film using BitTorrent, the swarm is in reality a collection of individual peers each of whom contributes much less than a substantial part of the film. I think it is arguable that the peers who participate in the distribution process make their individual contributions to the overall result pursuant to a common design and that it is through their concerted acts that the appellants' copyright is infringed: see *Morton-Norwich Products Inc v Intercen Ltd* [1978] RPC 501 at 515-516 per Graham J. However, the primary judge did not express his conclusion by reference to principles of joint tortfeasorship or common design and the appellants' case does not appear to have been advanced to his Honour in those terms. Nor did the appellants seek to uphold his Honour's analysis on that basis at the hearing of the appeal.

680 The appellants argued that the evidence showed that various individual RC-20 users electronically transmitted substantial parts of the appellants' films using BitTorrent. The best example of these from the appellants' standpoint was the RC-08 subscriber account. The evidence showed that this user had transmitted pieces of the film "Pineapple Express"

equivalent to about 8 seconds, 45 seconds and 47 seconds of footage. It was argued that this was likely to constitute a substantial part of the film.

681 The evidence does not disclose where these pieces of footage fit into the film as a whole. On the reasonable assumption that the relevant footage represents around one or two percent of the total length of the film (there was no evidence to suggest that it could be any greater than that), it is not possible to make a finding that the part or parts of the film transmitted represented a substantial part of the film without undertaking a qualitative assessment of some kind. Questions of both quality and quantity are relevant when determining whether a part of a film is a substantial part: *Network Ten Pty Limited v TCN Channel Nine Pty Limited* (2004) 218 CLR 273 at 293. I therefore reject the appellants' argument that this part, or any of the other part of a film relied upon for this purpose, was a substantial part of the whole.

ELECTRONIC TRANSMISSION FROM CLIENT TO SWARM

682 So far as communications between client and the swarm are concerned, the primary judge said, in a passage extracted above, that it could be assumed that "the viability of swarms relies on peers providing at least as much data as they take" and that it could be assumed that "peers not transmitting a substantial part of a film to the swarm must be the exception rather than the norm" (at [312]). On this basis his Honour concluded that iiNet users infringed the appellants' copyright by electronically transmitting the films. His Honour's analysis does not depend on treating the peer as a member of a swarm which transmits the whole of the film to another peer. Rather, it is based on an assumption (which I take to be a finding) that in the case of an electronic transmission made by an individual peer, a substantial part of the film is transmitted by the peer to the swarm.

683 The technical evidence relating to this question is mostly contained in a series of experts' reports by Mr Lokkegaard and Mr Carson who were called by the appellants to explain how BitTorrent and the DtecNet Agent worked. Their evidence, which was largely uncontroversial, does not support the finding made by his Honour. Nor is there any other evidence capable of supporting such a finding. Accordingly, I am not satisfied that the evidence established that individual iiNet users electronically transmitted either the whole or a substantial part of any of the appellants' films and I do not think his Honour's finding that

the whole of any particular film was electronically transmitted by iiNet users can be sustained.

THE EVIDENCE OF MR HERPS AND MR FRASER

684 I would also reject the appellants' argument that the evidence of the AFACT investigators, Mr Herps and Mr Fraser, established that individual iiNet users made electronic transmissions of substantial parts of the appellants' films. Both used internet connections provided to them by the respondent to download copies of various films using BitTorrent. However, it was not established by the evidence that the electronic transmissions which they received involved a substantial part of any of the films. I am mindful that the copies downloaded by Mr Herps and Mr Fraser were complete copies of the relevant films and that these were downloaded from swarms of iiNet users who made those films available online. But it was not established that any electronic transmission made to Mr Herps or Mr Fraser by any individual iiNet user (as opposed to a swarm) involved a substantial part of any such film. As to any electronic transmissions which may have been made by Mr Herps and Mr Fraser of the films downloaded by them, there was no evidence to show that any of these involved a substantial part of any of the relevant films.

Section 22(6) of the Act

685 The respondent argued that the evidence established that iiNet users who transmitted pieces of the appellants' films in response to requests issued by DtecNet did not electronically transmit such pieces because they did not determine the content of the relevant transmission: see s 22(6) of the Act. This argument must be rejected because it is factually incorrect and contrary to authority. The content of the relevant communication is determined by the person who responds to the request, not the person who makes it, because it is the person who responds to the request who determines the content of the response. The respondent's argument mirrors an argument that was put on behalf of the copyright owners in *Cooper* which was rejected by the trial judge but not relied upon in the appeal: see *Universal Music Australia Pty Ltd v Cooper* (2005) 150 FCR 1 at [69]-[74] per Tamberlin J.

"to the public"

686 Another issue raised by the respondent concerns the question whether the relevant electronic transmissions were made to the public. The primary judge said that it was not necessary for him to decide this question. With great respect to the primary judge, once it was found that there was an electronic transmission of the whole or a substantial part of any of the appellants' films, it was always going to be necessary to decide whether it was made to the public.

687 The respondent submitted that there was no electronic transmission to the public. It relied upon the decision of the High Court in *Telstra Corporation Ltd v Australasian Performing Right Association Ltd* (1996) 191 CLR 140 concerning the use of "music on hold" played for the enjoyment of Telstra customers waiting to have their calls to a service centre answered. The exclusive rights alleged to have been infringed were the right to broadcast the work and the right to transmit the work to subscribers to a diffusion service under s 31(1)(iv) and (v) of the Act as it stood prior to its amendment by the *Copyright Amendment (Digital Agenda) Act 2000* (Cth) (**the Digital Agenda Act**).

688 In *Telstra* Dawson and Gaudron JJ (with whom Toohey and McHugh JJ agreed) reviewed the authorities concerned with the right to perform a work in public including those concerned with performances occurring in private circumstances. After referring to the concept of the copyright owner's public, their Honours noted that the cases recognise that the relationship of the audience to the copyright owner is significant in determining whether there has been a performance to the public. Their Honours said (at 156-157):

> The distinction between what is "in public" and what is "in private" is of little assistance in determining what is meant by transmission "to the public". The transmission may be to individuals in private circumstances but nevertheless be to the public. Moreover, the fact that at any one time the number of persons to whom the transmission is made may be small does not mean that the transmission is not to the public. Nor does it matter that those persons in a position to receive the transmission form only a part of the public, though it is no doubt necessary that the facility be available to those members of the public who choose to avail themselves of it. …
>
> … Lying behind the concept of the copyright owner's public is recognition of the fact that where a work is performed in a commercial setting, the occasion is unlikely to be private or domestic and the audience is more appropriately to be seen as a section of the public. It is in a commercial setting that an unauthorised performance will ordinarily be to the financial disadvantage of the owner's copyright in a work because it is in such a setting that the owner is entitled to expect payment for the

> work's authorised performance …

689 Drawing upon the second of these passages in particular, the respondent argued that for a communication occurring in what it described as a "closed setting" to be a communication to the public, it was necessary for the communication to occur in a commercial context. The respondent argued that the communications shown to have taken place in the present case occurred in a closed setting and that none of the persons who made them was acting in a commercial context.

690 The key point made in *Telstra* is that in a private setting an unauthorised performance of a work will *ordinarily* be to the financial disadvantage of the copyright owner if it is at the same time made in a commercial setting because it is in such a setting that the copyright owner is entitled to expect payment for the authorised performance of the work. I do not think the relevant passage in the judgment supports the rather different proposition that it is *only* in a commercial setting that the copyright owner will suffer a financial disadvantage.

691 It was properly conceded by the respondent before the primary judge that iiNet users had infringed the appellants' exclusive right to communicate copyright material to the public by making it available online. It would be strange then if the transmission of that material to the members of that group who sought it out for the purpose of downloading it for their own use should be held not to involve a communication to the public. Yet that is the effect of the respondent's submission.

692 In the present case the question whether electronic transmissions made to or by iiNet users were to the public does not depend upon whether or not they occurred in a commercial setting. First, I do not think there was anything of a private or domestic nature about these communications. While the computers of many iiNet users may have been located in private homes, the transmissions were to whoever else happened to be part of the swarm. That could be anyone who had access to a computer with internet access. Secondly, I think it is reasonable to infer that the transmissions were to the financial disadvantage of the copyright owner. The iiNet users who downloaded copies of the appellants' films did so in circumstances where they not only paid nothing to the copyright owner for the privilege of obtaining their own copies of the appellants' films, but where they also made the appellants' films available online so that other internet users could do the same. Accordingly, had I

accepted that the iiNet users were shown to have electronically transmitted whole films or substantial parts of films using BitTorrent, I would have accepted that these were communications to the public.

Authorisation

693 The primary judge found that the respondent could not be held liable for copyright infringement by authorisation because it did not provide the primary infringers with the means with which they infringed the appellants' copyright. That conclusion must be read in the context of the facts upon which it was based. Importantly, while the respondent provided internet connectivity to users who infringed the appellants' copyright (including a modem and ancillary software to facilitate that connectivity) there was no suggestion, at a technical level, that it did any more than this. In particular, the respondent's facilities were not alleged to have been used to store copies of the appellants' copyright material. Nor was it alleged that the respondent supplied any of the additional hardware or software used to commit the primary infringements including, as the primary judge emphasised, the BitTorrent software.

694 Even so, the primary judge's reasons seem to imply that an ISP which provides internet connectivity will never be liable for authorisation of its subscribers' acts of copyright infringement because it could never be said that the ISP had supplied the means of infringement. With all due respect to the primary judge, I do not think that is correct.

695 The question whether an ISP is liable for authorising a person's infringing communication of copyright material using an internet connection supplied by the ISP depends upon a consideration of various factors including those to which the court must have regard to pursuant to s 101(1A). The primary judge's reasons make it clear that his Honour did not address those factors prior to concluding that the respondent was not liable for authorising acts of copyright infringement. He treated the question whether the respondent supplied the means of infringement as a threshold one which, if answered in the negative, was conclusive on the issue of authorisation. In the result, his Honour's consideration of the factors referred to in s 101(1A), and other matters which have previously been held to be relevant for this purpose, was a somewhat pointless exercise. In my view, his Honour erred in approaching the issue of authorisation in this way.

696 None of the authorities relied upon by the primary judge supports a threshold test of the kind applied by him. The primary judge relied heavily on the following statement of Gibbs J in *Moorhouse* (133 CLR 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 of copyright 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 that resulted from its use.

However, this cannot be understood as holding that a person will never be liable for authorisation unless he or she supplied the primary infringer with the means with which the acts of primary infringement were committed. Gibbs J also said (at 12) that "the question whether one person authorises another to commit an infringement depends upon all the facts of the case so that a decision on a particular set of circumstances may be of no assistance in other cases."

697 The question whether a person has supplied the means with which copyright has been infringed raises its own difficult issues. The primary judge concluded that the BitTorrent system was the means by which the appellants' copyright was infringed. But I cannot see why the means with which the primary infringers committed acts of infringement must be so narrowly defined. The primary infringers used computers which were no less essential to their infringing activities than was the BitTorrent system. The same is true of the internet connections with which they made the appellants' films available online.

698 The primary judge also referred to the Full Court's decision in *Cooper* in support of his view that the ISP was found liable in that case because it had, among other things, supplied the means of infringement. But their Honours did not adopt any threshold test of the kind postulated by his Honour. Further, his Honour's analysis of the facts in *Cooper* overlooks the fact that the ISP in that case did not supply the Mp3 files which the primary infringers made available online. Applying his Honour's reasoning, the Mp3 files in *Cooper* were the equivalent of the library books in *Moorhouse* yet the fact that they were neither supplied by the ISP nor stored on it servers did not prevent the Full Court from finding that the ISP had authorised the acts of primary infringement.

699 I have previously referred to other errors which the appellants sought to attribute to the primary judge's reasoning on the topic of authorisation. Because I am of the opinion that his Honour's approach to the issue of authorisation was affected by the error just discussed, it is not necessary for me to consider each and every one of the additional points raised by the appellants. But there are three particular matters which I will mention.

700 The first concerns the primary judge's conclusion that the contractual and technical power which the respondent possessed to terminate or suspend its services to subscribers was not a relevant power. I think this conclusion is incorrect. His Honour's approach to s 101(1A)(a) imposes a gloss on the words of the section. There may be some powers which may properly be regarded as irrelevant for the purposes of s 101(1A)(a) but I think the preferable view is that they are not powers at all for the purposes of s 101(1A)(a). Each of the contractual and technical powers was a power for the purposes of s 101(1A)(a). They could not be put aside on the basis that they were "not relevant".

701 The second matter concerns the primary judge's understanding of the words "sanction, approve, countenance" used in *Moorhouse* by Gibbs J (at 12) and Jacobs J (at 20). The primary judge said that those words must be read conjunctively. The respondent properly conceded that this was an error. Early in the development of this branch of law, the word "authorise" was said to mean "sanction, approve and countenance": *Falcon v Famous Players Film Co* [1926] 2 KB 474 at 491 per Bankes LJ. But within a short time of that decision these words were interpreted disjunctively: see, for example, *Copinger on the Law of Copyright*, 6th Edition (1927) by Mr F E Skone James at p 118 which states that "anyone who 'sanctions, approves or countenances' an infringement may be liable although the infringer is not his servant or agent." More recent statements of the law have been to this effect: see, for example, *Hanimex* 17 FCR at 288 per Gummow J, *Australasian Performing Right Association Limited v Jain* (1990) 26 FCR 53 (Full Court) at 61, *Nationwide News Pty Ltd v Copyright Agency Limited* (1996) 65 FCR 399 at 422 per Sackville J (with whom Jenkinson and Burchett JJ agreed), *Cooper* 156 FCR at para [20] per Branson J (with whom French J agreed).

702 I agree with the respondent's submission that this particular error is immaterial given that the primary judge went on to consider whether it could be said that the respondent had

sanctioned, approved *or* countenanced the acts of primary infringement. His Honour decided that the respondent did none of those things. But in the course of arriving at that conclusion his Honour made what I consider to be another error. He said that the words "imply a sense of official approval or favour of the infringements which occur" (at [501]). That proposition is inconsistent with *Moorhouse* in which Gibbs J said (133 CLR at 12) that "[e]xpress or formal permission or sanction, or active conduct indicating approval, is not essential to constitute an authorization." No doubt the University did not officially approve of Mr Brennan's act of copyright infringement but that did not prevent the Court inferring that his act was authorised by the University. As Gummow J reiterated in *Hanimex* (17 FCR at 286), the concept of authorisation is not confined to situations involving express or formal permission of some kind. Nor is it confined to situations involving official approval or favour of some kind.

Section 101(1) and (1A)

703 Branson J pointed out in *Cooper* (156 FCR at [20]) that the Digital Agenda Act, which introduced s 101(1A), did not reveal a legislative intention to alter the meaning of the word "authorise" in the context of the Act. But it did seek to guide determination of the relevant question by specifying a number of factors to which the decision maker must have regard in reaching a decision. Leaving aside the reference to any relevant industry code of practice in subsection (1A)(c), the other factors specified are ones that were taken into account in *Moorhouse* when it was held that the University authorised Mr Brennan's act of copyright infringement. As Kenny J said in *Cooper* (156 FCR at [136]), reference to *Moorhouse* assists in construing s 101(1A) because that section is premised on the concept of authorisation as developed by the High Court in that case.

Moorhouse

704 Apart from establishing that the word "authorises" as used in s 101(1) means "sanction, approve, countenance", *Moorhouse* also established that a person may authorise an act of infringement if he or she had some power to prevent it and knew or had reason to suspect that it might occur. This might be so where "[i]nactivity or indifference exhibited by acts of commission or omission … reach a degree from which an authorisation or permission may be inferred": *Moorhouse* 133 CLR at 12 per Gibbs J citing *Adelaide Corporation v*

Australian Performing Right Association Ltd (1928) 40 CLR 481 at 497-498, 503 per Higgins J. Jacobs J's reasons contain a statement to the same effect. His Honour cites the judgment of Bankes LJ in *Performing Right Society Ltd v Ciryl Theatrical Syndicate Ltd* [1924] 1 KB 1 at 9 which is central to the reasoning of both judgments in *Moorhouse* and the majority (including Higgins J) in *Adelaide Corporation*. Jacobs J added (133 CLR at 21) that "[i]t is a question of fact in each case what is the true inference to be drawn from the conduct of the person who is said to have authorised …".

705 Gibbs J found that the University had some power to prevent acts of infringement made possible by its provision of photocopiers and library books to students and that the University knew or had reason to suspect that such acts might be done. It was only after his Honour found that the precautions taken by the University to prevent acts of infringement from occurring were neither reasonable nor effective, that he went on to draw the inference that the University had authorised Mr Brennan's unlicensed reproduction of a substantial part of the relevant copyright work.

706 It would have been possible for the University in *Moorhouse* to deny people access to either the books or the photocopiers in the library. While this would have prevented them infringing copyright, it also would have prevented them from using the photocopiers to make copies in a way that did not involve any infringement of copyright. The question whether it would be reasonable for the University to deny people (who included students, staff and, as in Mr Brennan's case, ex-students) access to the library books or photocopiers was never expressly addressed by Gibbs J. His Honour instead asked what other steps the University could have taken to prevent infringement of copyright. Gibbs J relied, in particular, upon its failure to place on the photocopiers an adequate notice informing users that they were not to be used in a manner that would constitute an infringement of copyright. He described this as a "fatal weakness" in the University's case.

707 Jacobs J said that in the absence of any express permission, the real question was whether there was an invitation to be implied that Mr Brennan, in common with other users of the library, might make such use of the University's photocopying facilities as he saw fit. His Honour answered "yes" to that question and said (133 CLR at 21):

> The invitation to use is on the face of it an unlimited invitation. Authorization is

> given to use the copying machine to copy library books. It can hardly be said that the authorization is limited to the copying only of those books or parts of books which in the particular circumstances may be copied without infringement of copyright. In such a case knowledge of the prior doing of acts comprised in the copyright would not need to be proved nor would other positive or particular acts of invitation or authorization need to be shown.

His Honour also added (133 CLR at 22):

> In the circumstances it was of little importance whether or not the University authorities knew in fact that users of the machines were doing acts comprised in the authors' copyrights. This knowledge or lack of it would not change the terms of the invitation extended by the supply of books and machines. Knowledge could become important if the invitation were qualified in such a way as to make it clear that the invitation did not extend to the doing of acts comprised in copyright and if nevertheless it were known that the qualification to the invitation was being ignored and yet the University allowed that state of things to continue. Then it might be found as a fact that the University authorized the continued state of things, the continued use of its machines to do acts comprised in authors' copyrights, and thus to infringe those copyrights.

708 Like Gibbs J, Jacobs J did not address the question of what steps, if any, the University might reasonably be expected to take if properly worded notices were ignored by students. But neither judgment is inconsistent with the view that it might be appropriate for particular individuals who continued to infringe copyright in the face of such notices to be denied access to the library facilities to ensure that they did not continue to use them to infringe copyright.

Adelaide Corporation

709 The question which arose in *Adelaide Corporation* was whether the defendant had permitted its hall to be used for the public performance of the plaintiff's work (see s 2(3) of the *Copyright Act* 1911 (UK) as adopted by the *Copyright Act* 1912 (Cth)). Under the relevant statutory provision the defendant was liable if, for private profit, it permitted its hall to be used for such a purpose without the consent of the copyright owner, unless it proved that it was unaware, and had no reasonable grounds for suspecting, that the performance would be infringing. The defendant was the landlord of a hall which was to be used for a public concert during which various musical works were to be performed. The promoter of the concert (J.C. Williamson) was the occupier of the premises under a lease agreement made with the defendant. A letter was written on behalf of the copyright owner to the defendant advising that the performance was unauthorised and demanding that the defendant take steps

to ensure that the performance did not proceed. The question for decision was whether it could be said that the defendant had permitted the performance to occur by not taking steps to prevent the performance of the work in question by, if necessary, terminating the lease.

710 Higgins J's approach to that question involved asking whether the exercise of a power to terminate the lease was a reasonable step that might be taken for the purpose of preventing the performance taking place. The defendant had a contractual power to cancel the letting of the hall in which the performance of the copyright work was to occur not for any actual or threatened infringement of copyright, but in accordance with a broad power to terminate if the Town Clerk saw fit. This contractual power, if exercised, would have not only prevented the plaintiff's works being performed in the hall, it would have prevented the hall being used by the person to whom it had been let for any purpose. Higgins J said (at 40 CLR 498-499):

> [T]he plaintiff … relies … on clause 16 of the conditions of hire of the hall, which prescribes that the Town Clerk may, if in his judgment he thinks fit, cancel the letting, returning the deposit and the rent for the unexpired term. That is to say, that, as the Corporation has no power to prevent directly the singing of the song, it should smash the lease, refunding money paid for all future performances of every kind, and thus prevent all singing of any sort. This seems rather an extreme suggestion...
>
> Is the smashing of the lease a "reasonable step" under the circumstances? It is 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.

711 Since the power to terminate the lease was not one which Higgins J considered that the landlord could reasonably be expected to exercise in response to the letter of demand, his Honour was not prepared to hold that the landlord had permitted the infringing performance. Gavan Duffy and Starke JJ, who with Higgins J made up the majority, approached the question rather differently. After referring to the power to cancel the letting agreement contained in clause 16 of the relevant conditions, their Honours said (at 504-505):

> Despite the notice given to the Corporation, it neither exercised this power nor took any step to induce the hirer to prevent the performance. Now, the clause does not give the Corporation any control over J. C. Williamson Ltd. or Hislop or over concerts given by them in the Town Hall: all it authorizes is a termination of the contractual relationship constituted by the letting agreement. The failure to prevent that which a man can legally prevent may be evidence of his consent to its coming into, or continuing in, existence; but no inference of consent should be drawn against one who having no such right remains quiescent and declines to alter his legal relations in order to acquire such a right.

712 The respondent relied upon *Adelaide Corporation*, particularly the judgment of Higgins J, when seeking to uphold the primary judge's conclusion that the respondent did not have any relevant power to prevent copyright infringement. However, *Adelaide Corporation* concerned a quite different statutory provision to that now under consideration and it has, in any event, been overtaken by the High Court's subsequent decision in *Moorhouse*. There are also clear differences in reasoning among the majority. Nevertheless, there is one observation that I would make arising out of *Adelaide Corporation* which I see as having particular relevance to the appeal.

713 When addressing s 101(1A)(a), the Court does not merely ask whether a person has a power to prevent the doing of the relevant act. It must also evaluate the extent of that person's power. While I disagree with the primary judge's interpretation of s 101(1A)(a), I accept that the question whether it would be reasonable for a person to exercise such power as he or she is found to have is a relevant consideration. In weighing up this consideration it may sometimes be useful to ask whether the power is a direct or an indirect power to prevent the doing of the relevant act. As Higgins J emphasised, the landlord in *Adelaide Corporation* had no direct power to prevent the performance of the plaintiff's work in the sense that it could only prevent the unauthorised performance of the plaintiff's work by bringing the lease to an end. All other things being equal, the more direct a person's power to prevent copyright infringement, the greater the likelihood that the failure to exercise it will result in a finding of authorisation.

Other authorities

714 There are several cases decided after *Moorhouse* which are relevant to issues arising in this case. A number are concerned with "home taping" technology and the secondary liability of manufacturers or suppliers of products used to make copies of films or sound recordings.

715 In *Australian Tape Manufacturers Association Ltd v Commonwealth* (1993) 176 CLR 480 the High Court considered whether the seller of a blank audio tape was liable for authorisation of copyright infringement. In their joint reasons for judgment, Mason CJ, Brennan, Deane and Gaudron JJ referred with apparent approval to the decisions of the House of Lords in *CBS Songs Ltd v Amstrad Consumer Electronics Plc* [1988] AC 1013 and

the Supreme Court of the United States in *Sony Corporation of America v Universal City Studios Inc* (1984) 464 US 417. Their Honours said (at 497) that "[t]he sale of a blank tape does not constitute an authorization by the vendor to infringe copyright … principally because the vendor has no control over the ultimate use of the blank tape." Nor did it matter that the vendor knew that there was a likelihood that the article would be used to infringe copyright. The authorities cited by them in support of this proposition included *Moorhouse* and *Hanimex*. Their Honours also said (at 498):

> It 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 the article. It was the absence of such control in *C.B.S. Songs Ltd*. that constituted the critical distinction between the decision in that case and the decision in *University of New South Wales v. Moorhouse*, where the University had power to control what was done by way of copying and not only failed to take steps to prevent infringement but provided potential infringers with both the copyright material and the use of the University's machines by which copies of it could be made. Accordingly, in *Moorhouse*, authorization was made out.

(citations omitted)

716 It can be seen that there were two factors referred to by their Honours which were crucial to their analysis. The first was that the articles in question had lawful uses. In that regard, their Honours had earlier quoted Stevens J in *Sony* who had said that there could be no infringement if the product sold was "capable of substantial non-infringing uses". The second was that the vendor of the article in question had no control over the purchaser's use of it. I think it is reasonably apparent that their Honours were referring to the need for there to be *some* element of control over the purchaser's use of the product subsisting at the time of the commission of the primary act of copyright infringement.

717 Unlike the primary judge, I do not understand Branson J's remarks in *Cooper* (156 FCR at [41]) to be inconsistent with anything said in *Australian Tape Manufacturers*. In *Cooper*, the first respondent (Mr Cooper) could have disabled the website established and maintained by him at any time. He therefore had power to prevent the infringements of copyright that occurred when visitors to his website clicked on links to Mp3 files that he allowed others to establish there. Her Honour's remarks were made in the course of rejecting a submission that because Mr Cooper's website was designed in such a way that he had no

immediate control over the use of links on his website while it remained live, he had no power to prevent. That is not inconsistent with anything said in *Australian Tape Manufacturers*.

718 In *Hanimex*, which was also concerned with the promotion and sale of blank audio tapes, Gummow J said (17 FCR at 286):

> The question has then arisen, as in the United States, of what degree of connection or control is necessary between the alleged authoriser and the primary infringer, particularly where the primary infringer has used equipment made available or supplied by the alleged authoriser or that party has provided equipment used in conjunction with other equipment to effect the primary infringement. Thus, in *Moorhouse's* case (supra) the controversy surrounded the use of photocopying machines made available in the university library, and in *CBS Incorporated v Ames Records and Tapes Ltd* [1982] Ch 91, the defendant had set up a "library" for the lending of records for a fee to members of the public who allegedly used the records to make unauthorised copies on "home-taping" equipment. In the latter case the defendant was not liable for "authorisation"; the result no doubt would have been different if the re-taping had taken place on the defendant's premises with a machine made available by him: *RCA Records v All-Fast Systems Inc* 594 F Supp 335 (1984).

His Honour went on to say that it was unnecessary to express any general view as to what is the necessary element of connection or control which must exist for there to be an authorisation. But in any event, the question of how much power must exist for there to be authorisation cannot be looked at in isolation. It will depend on a variety of other factors relevant to the question of whether there has been an authorisation including whether it is reasonable or practical that such a power be utilised for that purpose. As the authorities repeatedly emphasize, it is in every case necessary to decide what inference is to be drawn from the conduct of the person who is alleged to have authorised another person's copyright infringement. Can it be inferred that the person concerned has approved, sanctioned or countenanced the primary infringement?

Section 101(1A)(a) - the extent (if any) of the respondent's power to prevent the doing of the act concerned

719 The first matter which s 101(1A)(a) requires the Court to take into account is the extent (if any) of a person's power to prevent the doing of the act concerned. In a case founded on allegations of inactivity or indifference, authorisation can only occur where a person has some power to prevent the act of infringement occurring. The words "if any" which appear in parenthesis in s 101(1A)(a) are not inconsistent with that proposition. They

recognise that there will be other types of cases which are not founded on inactivity or indifference where the person has engaged in positive acts which justify a finding of authorisation. Gummow J in *Hanimex* (at 286) referred to those cases which involve a purported exercise of power or a purported exercise of authority which does not actually exist. There are also those cases in which a person can be said to have intentionally induced or encouraged another person to infringe copyright.

720 The respondent has the technical power to prevent copyright infringement by iiNet users by denying them access to the internet using the respondent's facilities. Clause 14.2(j) of the CRA provides that the respondent may, without liability, immediately cancel, suspend or restrict the services it provides to a subscriber if the respondent reasonably suspects "illegal conduct" by the subscriber or any other person in connection with such services. In this context, the expression "illegal conduct" refers to conduct that is contrary to or forbidden by law. There is no dispute that this includes copyright infringement. Thus, the respondent has a contractual power to cancel, suspend or restrict its services to a subscriber if it reasonably suspects that they are being used by any person (not merely the subscriber) to infringe copyright. This gives the respondent a wide legal power with which to justify the use of its technical power to terminate or suspend a subscriber's internet access in appropriate cases. It is the combination of these technical and legal powers which comprise the power of the respondent to prevent iiNet users from making the appellants' films available online.

721 There are some further observations I would make concerning the nature and extent of this power at this stage of the analysis.

722 First, the power to terminate or suspend is not one that gives the respondent any direct control over what materials a user of its network may make available online, access online, download or copy. By contrast, it was open to the University in *Moorhouse* to withdraw particular books from the library or to forbid any, or any extensive, photocopying of them. I think this is an important point which the primary judge was right to emphasize although, as I have explained, it is not determinative and must be considered along with all other relevant matters.

723 Secondly, a termination or suspension of services deprives the customer of his or her internet facilities. On the evidence, it is not within the power of the respondent to deny iiNet

users access to particular copyright material found on the internet short of denying them access to the internet as a whole. Hence, while the respondent has power to prevent its internet facilities from being used to infringe copyright, this is only achieved by preventing them from being used for any purpose.

724 Thirdly, the contractual power to terminate or suspend is an ample one and the respondent is given a wide discretion. It need only suspect, on reasonable grounds, that its services have been used to infringe copyright for the discretion to be enlivened. Nevertheless, that does not mean that the commercial decision as to whether or not to terminate a particular account is necessarily a simple one.

725 The circumstances in which the power to terminate is enlivened can range from a situation in which the respondent knows that the connection is being used wholly or substantially for infringing purposes to one where the respondent reasonably suspects that it has been used to commit an isolated and innocent act of infringement. The kinds of situation in which the commercial decision might be considered a simple one would include, at what is admittedly the most extreme end of the spectrum, one in which the respondent actually knew that a particular customer's account had been used wholly or substantially for the purpose of infringing copyright. It was not established that any of the RC-20 accounts had been used wholly or substantially for the purpose of infringing copyright.

Section 101(1A)(b) – the nature of any relationship existing between the respondent and the person who did the act concerned

726 The second matter which s 101(1A)(b) requires the Court to take into account is the nature of the relationship between the respondent and the person who did the act concerned.

727 The relationship between the respondent and its subscribers is one pursuant to which the respondent, in return for what will usually be fixed monthly fees, provides the connectivity which enables users to access the internet. The relevant relationship for the purposes of s 101(1A)(b) may or may not be contractual depending upon whether the person who committed the act of infringement is one of the respondent's subscribers. If he or she is a subscriber, then the relationship is one that is governed by the terms of the CRA. Even if the relationship is not contractual, in the sense that the user of the service is not the subscriber,

then it is, in any event, closely akin to contractual in that the user's right to use the respondent's service could never rise any higher than that of the subscriber.

728 Clause 4.2 of the CRA provides (inter alia) that the subscriber must not use, or allow anyone else to use, the respondent's service to infringe another person's rights (sub-para (a)) or for any illegal purpose or practice (sub-para (e)). Hence, the contractual arrangements pursuant to which the respondent makes its services available to its subscribers expressly forbid the subscriber from engaging in, or allowing any other person to engage in, any of the acts of copyright infringement which the respondent is alleged to have authorised.

Section 101(1A)(c) – whether the respondent took any other reasonable steps to prevent or avoid the doing of the act including whether it complied with any relevant industry codes of practice.

729 The matter which s 101(1A)(c) requires the court to take into account is whether the respondent took any other reasonable steps to prevent or avoid the doing of the act of infringement including whether the respondent complied with any relevant industry codes of practice. It is common ground that there are no relevant codes of practice.

730 The word "other" as used in s 101(1A)(c) is curious because neither of the preceding sub-paragraphs identify anything in the nature of a "step". While it is important to give meaning to all the words used in s 101(1A) where possible, it is difficult to resist the conclusion that the use of the word "other" in s 101(1A)(c) is a drafting error.

731 The respondent relied upon a series of steps which it says it took to prevent or avoid copyright infringement by users of its network. These steps included:

- making its services available to customers and other users upon terms which prohibited them from using such services to infringe copyright;
- publishing a warning on its website that the hosting or posting of infringing material using the respondent's network was a breach of the CRA which could result in the suspension or termination of a customer's account;
- providing training and instruction to employees to the effect that the respondent does not support or condone copyright infringement.

It may be accepted that these steps, so far as they go, were reasonable steps to take to prevent or avoid copyright infringement by users of the respondent's network. But, of course, it does not follow that the steps relied upon by the respondent, considered as a whole, were adequate for that purpose or that there were no other reasonable steps that it was also open to the respondent to take.

732 The appellants gave particulars of the steps which they alleged the respondent failed to take but could have taken to prevent or avoid the relevant acts of infringement. The relevant paragraph of the appellants' particulars is in these terms:

> The steps which iiNet could have taken include:
>
> (a) sending a notice or email to iiNet Customers warning them that their iiNet Internet Services had been identified as being used to infringe copyright;
>
> (b) notifying iiNet Customers that their conduct (or the conduct of those users of the account) involved a breach of the *Customer Relationship Agreement*;
>
> (c) requesting that the iiNet Customers or other customers of the account cease such conduct;
>
> (d) warning iiNet Customers that if such conduct continued their iiNet Internet Services would be disconnected, suspended or terminated;
>
> (e) repeating the steps in (a) to (d); and/or
>
> (f) disconnecting, suspending or terminating iiNet Customers' iiNet Internet Services.

733 It was not suggested by the appellants that the respondent should monitor transmissions made via the internet connections provided to its subscribers with the intention of ascertaining which of them might have engaged in copyright infringement. Nor was it suggested that such transmissions should be filtered with the intention of preventing or avoiding copyright infringement. As is apparent from the particulars, the focus of the appellants' case at trial, at least in so far as s 101(1A)(c) is concerned, was on the respondent's failure to notify, warn, terminate and disconnect subscribers whose accounts had been identified as being used to infringe copyright.

734 Having referred to the particulars given by the appellant, it is necessary to return to some of the primary judge's findings. His Honour referred to "[o]ther technical mechanisms" (ie. apart from the power to warn and then terminate or suspend) which he said were referred to from time to time but which his Honour put aside on the basis that there was inadequate

evidence concerning their scope or effectiveness. On the view I have come to nothing turns on these matters but I will, in any case, explain why I think the primary judge's assessment of this evidence was correct.

735 During the hearing of the appeal the appellants stated that they no longer rely on website "blocking" but that they do rely on "shaping" and "play penning" as technical measures that the respondent could adopt to prevent or avoid acts of copyright infringement. Of these, the latter, but not the former, was expressly rejected by the primary judge for lack of evidence. According to Mr Cobden SC, shaping was hardly touched on in the submissions made to the primary judge. This may explain why his Honour does not expressly deal with it.

SHAPING

736 In the appeal, the appellants submitted that shaping is a reasonable step, short of terminating or suspending a subscriber's account, that the respondent could take to prevent or avoid copyright infringement by people who use its facilities for that purpose. It involves the intentional slowing down of the connection speed for a particular account.

737 Mr Malone gave evidence at the trial concerning shaping. It is apparent that he did so for the purpose of showing that the respondent took steps to reduce subscribers' connection speeds in order to discourage use in excess of allotted download quotas. His evidence in chief on this topic was relevantly as follows:

> Shaping refers to the slowing of a connection that has exceeded its allotted download allowance for a period of time. The connections are reduced from 0.5 Mbps to 12.8 Mbps (depending on the speed of the connection) to about 64kbps. The following are examples of download times at various speeds of various sizes of file, using the nominal clock speeds; real time would be about 15% longer due to congestion, errors, retries, etc:

Size of File	**Example**	**Time at 12 Mbps**	**Time at 5 Mpbs**	**Time at 64kpbs**
1 Gigabyte	High Definition Feature Film	10 to 15 minutes	25 to 30 minutes	30 to 40 hours
250 Megabytes	40 high quality photographs (e.g. a travel album)	2 to 3 minutes	6 to 7 minutes	8 to 9 hours

> As a result, the subscriber's connection speed is extremely slow and the

> subscriber is to a large degree limited in the ways they can use their Internet access service. For example, streaming (e.g. from news sites) of video clips becomes impractical …
>
> ISPs who do not use shaping result in the possibility of Internet users receiving large and unexpected bills at the end of a month. In the days when shaping was less common, this included, of course, parents of children who were using the Internet and the like. Unexpectedly large bills were a major issue in terms of customer relations. Once shaping was introduced, the phenomenon of unexpectedly large bills ceased to be such a problem …

738 Mr Malone was cross-examined on the topic of shaping quite briefly. The appellant referred us to this particular exchange in Mr Malone's cross-examination:

> And you've told us how the customer's account can be shaped, speeds slowed down, at will by iiNet --- Not at will, but yes.
>
> Well, at will in the sense that if it wanted – technically wanted – it has a technical ability to do it? --- Yes.
>
> You say it will only do it in circumstances where the quota is approaching? --- Yes

739 The appellants also referred us to various documents which did no more than confirm that the respondent could shape a subscriber's account once its limit was exceeded.

740 Thus, the evidence of Mr Malone established that the respondent regularly shapes accounts which exceed their quota to discourage excessive use. The respondent argued, on the basis of Mr Malone's evidence, that shaping accounts helps to discourage acts of infringement simply because it discourages excessive use. The logic of that argument can be put to one side. What is most relevant for present purposes, is that the question whether it would be feasible to shape accounts which do *not* exceed their quota was not explored in the evidence. In circumstances where the appellants' particulars made no mention of shaping, I would hesitate to act on what appears to be the very slender material on which the appellants now rely. It was for the appellants to establish that shaping was a reasonable step which the respondent could have taken to prevent or avoid iiNet users engaging in copyright infringement. I do not think that they have done so.

PLAY-PENNING

741 The appellants also relied upon "play-penning" as another reasonable step, short of terminating or suspending a subscriber's account, that the respondent could take to prevent or avoid copyright infringement. It involves restricting a subscriber's access to a small number

of sites. The primary judge explicitly rejected play-penning as a reasonable step which the respondent could have taken to prevent or avoid acts of copyright infringement by iiNet users on the basis of "insufficient evidence". I think his Honour was correct to do so.

742 Again, the particulars given by the appellants made no reference to the ability of the respondent to play-pen iiNet customers for the purpose of preventing or avoiding copyright infringement. So I begin by referring to the appellants' written submissions in chief where this matter is only briefly taken up:

> [35] iiNet had a range of technical measures available to it including … play-penning … The evidence ought to have led his Honour to conclude that these measures were available and could have been used by iiNet to prevent infringement.
>
> [80] … Internal records showed that iiNet had already made far-reaching changes to the systems that applied "playpenning" to introduce a capacity to direct users to problem – specific web pages and to disconnect a user during an online session. iiNet did not explain why these systems could not be used in conjunction with copyright warnings.

743 The first of the references given in these parts of the written submissions refer to the following evidence in the cross-examination of Mr Malone:

> You accept that measures are available to iiNet to playpen customers by limiting access to certain sites?---So it literally removes the rest of the internet and just restricts them to a small number of sites?
>
> Yes?---Yes.
>
> And one of those facilities is used to enable – limit a customer's access only to iiNet's website, which enables them to make a payment on their account?---Yes.
>
> In other words, their access to the net – there's a capacity in iiNet to limit the access of a customer who is not paying their bills to only one site on the web, namely a site enabling to make payment?---Yes
>
> And that's – the description of that tool is playpenning the customer, or playpenned? ---Yes

744 The second piece of evidence referred to is a document described as "Project Design Document" entitled "User Playpen (ISG) Revision 0.7". The first draft of this document appears to have been created in June 2008 but since it was not in evidence it is not possible to know what form it then took. The version of the document that was in evidence is dated 27 November 2008 which is subsequent to the commencement of the proceeding. Significantly, the document does not refer to any existing system of play-penning. Rather, it

refers to what were, as at November 2008, various technical possibilities involving a "high level design for integrating play-pen/walled garden functionality". Mr Malone gave his evidence in November 2009 and the system of play-penning referred to in his oral evidence on which the appellants rely would appear to be one that was not developed until sometime in that year. How long before November 2009 the system was developed is not apparent from his or any other evidence.

745 Mr Catterns QC, who appeared for the appellants on the appeal, did not refer us to any other evidence relevant to this topic beyond that referred to in the written submissions to which I have already referred. I therefore agree with the primary judge that there was insufficient evidence to establish that, at relevant times, play-penning was a reasonable step which the respondent could have taken to prevent or avoid iiNet users engaging in copyright infringement.

WARNING, SUSPENSION, TERMINATION

746 This brings me to the failure of the respondent to take any of the steps specified in the particulars in response to the AFACT notices. The appellants highlighted the respondent's failure to take any such steps by comparing it to the respondent's willingness to act against a subscriber who fails to pay amounts payable under the CRA. In such cases warning notices, followed (if necessary) by termination and disconnection, are steps routinely taken by the respondent to enforce payment.

747 The primary judge seems to have come to the conclusion that the giving of a warning could not be a reasonable step for the purposes of s 101(1A)(c) because the mere giving of a warning is not a power to prevent. I would accept that the ability to give a warning is not in itself a power to prevent for the purpose of s 101(1A)(a). However, s 101(1A)(c) is concerned with a different matter namely, what "reasonable steps" the alleged authoriser might have taken to prevent or avoid any of the relevant acts of copyright infringement.

748 I am satisfied that the primary judge erred in holding that the giving of a warning could not be a reasonable step that might be taken to prevent or avoid the relevant acts of copyright infringement. If the ability to give a warning is supported by a power to terminate

or suspend a subscriber's account then there can be no doubt that the giving of a warning is capable of amounting to a reasonable step for the purpose of s 101(1A)(c).

749 Nor do I think that the difficulties involved in establishing a system for giving warnings and, if necessary, termination or suspension of accounts, were likely to be as great as Mr Malone's evidence might suggest. It is true that the respondent, if it was to take the step of issuing warnings in particular cases, would need to decide when it would be appropriate to do so. To that end, the respondent would need to decide, among other things, whether the available material was sufficient to satisfy itself that it was appropriate for a warning to be issued or for an account to be terminated. It is also true that the respondent would need to decide how many warnings should be given (unless it decided that no warnings need be given) before terminating or suspending service to a particular subscriber. These and like questions involve matters of judgment and degree. As I have already acknowledged, the decision as to whether or not to terminate a particular account may not be a simple one. But I do not accept that the adoption of some system providing for the issuing of warnings followed by termination or suspension is not a reasonable step which the respondent could have taken for the purpose of preventing or avoiding copyright infringement by users of its network.

750 Nevertheless, in the absence of applicable regulations or access codes which might guide an ISP's decision making in relation to such questions, it seems to me that an ISP should be given considerable latitude when working out the detail of such a system. It is always possible to argue that a system for the issue of warnings and termination could be tougher than it is. But it would be difficult to criticise an ISP on that account if it acted in good faith to devise and implement a system that involved taking such steps against subscribers who the ISP was satisfied had used (or permitted others to use) its facilities for the purpose of committing flagrant acts of copyright infringement.

751 In my opinion it was open to the respondent to adopt a system providing for the issuing of warnings and, if appropriate, the termination or suspension of accounts where the respondent was satisfied that a subscriber's account had been used to infringe copyright. The respondent had no such system in place. It did not even have a system that provided for the giving of a warning to a subscriber who it was satisfied had knowingly and repeatedly

engaged in copyright infringement on a widespread scale. The absence of such a system is a matter that is made relevant by s 101(1A)(c).

Other relevant matters

ENCOURAGEMENT OF INFRINGEMENT

752 Before the primary judge, the appellants argued that the respondent intended that iiNet users engage in copyright infringement, that the respondent profited from copyright infringement and that it was in the respondent's commercial interest that copyright infringement continues to occur across the respondent's network. The primary judge's rejection of each of these propositions is not challenged in the appeal. The appellants also argued that the respondent encouraged iiNet users to engage in copyright infringement. Again, this argument was rejected by the primary judge though the appellants maintain that his Honour was wrong to reject it. They rely upon a press release and a radio advertisement which they say show the respondent actively encouraging users to engage in copyright infringement.

753 The press release relied upon by the appellants was issued on behalf of the respondent on the day the appellants commenced the proceeding against the respondent. It refers to the respondent's intention to defend the proceeding and expresses the view that the AFACT notices were not sufficient to require it to disconnect any iiNet user's service. The press release also states that "iiNet does not in any way support or encourage breaches of the law, including copyright infringement" and that iiNet "had repeatedly passed on copyright holders' complaints to law enforcement agencies for investigation".

754 I do not think it could be said that notifying the public in this way that iiNet would refer any complaints regarding copyright infringement to the police shows that the respondent was encouraging copyright infringement. Similarly, I agree with the primary judge that the fact that this press release was made available for download from the respondent's website in two formats, one of which was by BitTorrent, does not lead to any different conclusion.

755 The radio advertisement relied upon by the appellants was referred to by the primary judge as the "Golden Girls advertisement". The transcript of the advertisement is in the following terms:

> [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.

The vice with this advertisement was said to be that since episodes of the television program *The Golden Girls* were not available for authorised download, the advertisement implied that iiNet's services could still be used to download such episodes from unauthorised sources. On this issue I agree with the primary judge. The advertisement appears to have involved an attempt at humour. I do not think there is any substance in the suggestion that it would have encouraged iiNet users to download unauthorised copies of the Golden Girls or to engage in other acts of copyright infringement.

756 The appellants also argued that by failing to take steps to prevent or avoid copyright infringement by iiNet users the respondent had encouraged such conduct. There is no doubt that the respondent's failure to take reasonable steps to prevent or avoid copyright infringement is, as previously explained, a relevant matter which must be taken into account. However, I do not think the failure to take such steps merits any separate or different consideration on the basis that it somehow amounts to encouragement to infringe. It would be another matter if the acts of encouragement relied upon showed that the respondent had incited or induced iiNet users to infringe but, in the present case, the omissions relied upon by the appellants in support of its argument have a different character.

KNOWLEDGE OF INFRINGEMENTS

757 As the primary judge pointed out, the respondent accepted that it had general knowledge of copyright infringement committed by iiNet users. But as he also observed, it would be difficult for the respondent to act on knowledge of such a general kind with a view to preventing or avoiding copyright infringements by people using its network. This is because the respondent would have no means of knowing who had used its facilities to infringe copyright unless that knowledge was provided to it by third parties. However, the appellants submitted that the AFACT notices provided the respondent with all it needed to know to issue warnings to iiNet subscribers and, if appropriate, terminate or suspend the accounts used to infringe copyright. For reasons which I will explain, I do not think that is correct.

758 To the extent that the respondent might become aware of specific acts of copyright infringement in which its subscribers were allegedly involved, the respondent could only be expected to acquire such knowledge, for all practical purposes, as a consequence of notices received from third parties, most likely copyright owners or their representatives, who engaged in some form of electronic surveillance. Such notices necessarily relate to events which have occurred in the past which the respondent is not able to independently confirm without considerable difficulty.

759 As I have previously mentioned, the primary judge was critical of the AFACT notices. He said that AFACT should have explained in detail how the DtecNet Agent operated so that the respondent could understand how the copyright infringement allegations came to be made. There was evidence, which the primary judge appears to have accepted, that at least some of the surveillance and detection methods previously employed on behalf of film studios and record companies against users of peer to peer technology had been shown to be unreliable. His Honour's observation that the AFACT notices should have explained how the relevant data was collected must be understood against that background.

760 The regulations made for the purposes of the safe harbour provisions include a prescribed form that is designed to help safeguard the interests of ISPs who are the subject of "take down" notices issued by or on behalf of copyright owners who claim that material stored on the ISP's system or network is infringing material. Though these regulations have no direct application in the present circumstances, they still provide a useful illustration of what an ISP might reasonably expect to receive from a copyright owner who asserts that the ISP's facilities are being used for the purpose of copyright infringement.

761 In particular, the prescribed form requires a copyright owner or his or her agent to declare that the owner or agent believes, in good faith, that the material stored by the ISP is an infringement of copyright and that the copyright owner has taken reasonable steps to ensure that the information and statements in the notice are correct: see Schedule 10, Part 3 of the *Copyright Regulations* 1969 (**the Regulations**). A note is also included on the form which states that it is an offence under the *Criminal Code* to issue such a notice knowing that it is false or misleading in a material particular: see s 137.2 of the *Criminal Code Act* 1995 (Cth).

762 While there is room for argument about the level of detail that the AFACT notices might have contained, it is clear that they did not contain any explanation of how the DtecNet Agent operated. Nor did they contain any statement verifying the accuracy of the data or the reliability of the methods used to collect it.

763 In my opinion the AFACT notices were not sufficient to provide the respondent with knowledge that its network was being utilized by users of particular accounts to infringe the appellants' copyright in the identified films. I accept that they must have given the respondent reason to suspect that such infringements had occurred. However, knowing that specific acts of copyright infringement have occurred and merely suspecting that they have occurred are quite different things. In the circumstances of the present case, the difference is of considerable significance.

764 It is important to recall, as the primary judge found, that the respondent has hundreds of thousands of customers and that each day it receives hundreds of notices issued by or on behalf of copyright owners. I do not think the respondent could reasonably be expected to issue warnings, or to terminate or suspend particular accounts, in reliance upon any such notice in circumstances where it has been told nothing at all about the methods used to obtain the information which lead to the issue of the notice. Nor should it be up to the respondent to seek out this information from a copyright owner who chooses not to provide it in the first place.

765 The respondent was never told how DtecNet Agent operated until sometime after February 2009 when the appellants' experts' reports were served. Mr Malone's evidence suggests that he first became aware of how DtecNet operated in April 2009 after an expert engaged on behalf of the respondent had considered those reports. It is true that the appellants' amendments, to which I previously referred, were not made until May 2009. Nevertheless, I do not accept that knowledge acquired by the respondent by way of expert reports served prior to the trial could be used for the purpose of establishing that the respondent knew what the DtecNet's methods were, or that they were reliable, or likely to be reliable, at least not in circumstances where, as I understand them, the experts' reports were the subject of both express and implied confidentiality restrictions which would have prevented them from being used other than for the purposes of the proceeding.

766 The appellants also submitted that the respondent was "wilfully blind" to the matters disclosed in the AFACT notices which I take to mean that the respondent deliberately abstained from inquiring into those matters for fear of what the inquiry might reveal: *Colbeam Palmer Ltd v Stock Affiliates Pty Ltd* (1968) 122 CLR 25 at 33 per Windeyer J. In determining whether a person should be taken to know of facts on the ground that he or she was "wilfully blind" to them, it is necessary to look to the motivation behind the failure to make inquiry. In *The Queen v Crabbe* (1985) 156 CLR 464 at 470-471 the High Court approved the following statement by Professor Glanville Williams in *Criminal Law: The General Part*, 2nd ed. (1961) at 159:

> A court can properly find wilful blindness only where it can almost be said that the defendant actually knew. He suspected the fact; he realised its probability; but he refrained from obtaining the final confirmation because he wanted in the event to be able to deny knowledge. This, and this alone, is wilful blindness. It requires in effect a finding that the defendant intended to cheat the administration of justice.

767 In the present case the explanation behind the respondent's failure to make inquiry is much less sinister. Rightly or wrongly, it was the respondent's view that it was not obliged to go to the effort and expense of making any inquiries in response to the AFACT notices. I do not think the concept of wilful blindness assists the appellants' case.

"INACTIVITY OR INDIFFERENCE"

768 The appellants argued that the evidence before the primary judge revealed a level of inactivity and indifference on the part of the respondent towards copyright infringement by iiNet users that should have led his Honour to infer that the respondent authorised the primary acts of copyright infringement. There are a number of observations I would make concerning this argument.

769 First, the inactivity relied upon was the failure of the respondent to take steps to issue warnings and, if appropriate, terminate or suspend particular accounts in response to the AFACT notices. It was not suggested that the respondent was under any legal obligation to respond to the AFACT notices in this way. The question is whether its failure to do so supports the drawing of an inference that the respondent approved, sanctioned or countenanced the relevant acts of copyright infringement.

770 Secondly, the appellants sought to demonstrate that the respondent was indifferent to iiNet users acts of copyright infringement by reference to various internal communications between officers of the respondent including Mr Malone and Mr Dalby. While these communications were often expressed in colourful terms, they were mostly to the effect that the respondent was not required to act on the AFACT notices. These communications may reflect indifference of a kind, but the question is whether it is the indifference of someone who approves, sanctions or countenances other people's acts of copyright infringement.

771 Thirdly, it is impossible to ignore his Honour's acceptance of much of the evidence of Mr Malone and Mr Dalby who he essentially found to be honest and reliable witnesses. In particular, the primary judge accepted Mr Malone's evidence that the respondent did not approve of iiNet users engaging in copyright infringement.

772 I have already referred to the appellants' abandonment of the ground of appeal which directly challenged his Honour's acceptance of Mr Malone's evidence. Ultimately, the appellants never really confronted this evidence or his Honour's acceptance of it beyond referring to his Honour's observation that the words "approve, sanction, countenance" imply some form of "official approval or favour". Yet Mr Malone's evidence that the respondent did not approve of iiNet users infringing copyright was not the subject of any such qualification and there is no reason to think that the primary judge interpreted his evidence as though it was.

773 The primary judge also rejected any suggestion that the appellants "tacitly approved" of copyright infringement by iiNet users.

774 In *Hanimex* (17 FCR at 256) Gummow J referred to the decision of Whitford J in *CBS Incorporation v Ames Records and Tapes Ltd* [1982] Ch 91 which was another of the home taping cases. Whitford J, after referring to the judgment of Bankes LJ in *Ciryl*, said (at 112) in answer to a submission made by Mr Laddie QC in reliance upon (inter alia) the High Court's decision in *Moorhouse*:

> But of course the question so far as the point of indifference is concerned goes back really to what Bankes L.J. said about the matter. Is this again a case of the indifference of somebody who did not consider it his business to interfere, who had no desire to see another person's copyright infringed, but whose view was that copyright and infringement were matters in this case not for him, but for the owners

> of the copyright? It must be recalled that the most important matter to bear in mind is the circumstances established in evidence in each case.

775 It follows from the findings of the primary judge that the position of the respondent did not reflect any intention or desire to see the appellants' copyright infringed. Rather, it reflected a view, strongly held it would seem, that it was not the business of the respondent to be taking action against subscribers on the basis of allegations of copyright infringement contained in the AFACT notices. None of that is to say that the respondent's view on the matter was necessarily correct. But it cannot be dismissed or discounted on the basis that it was either not genuinely held or not reasonably open.

Did the respondent sanction, approve or countenance copyright infringement?

776 This brings me to the critical question which is whether it should be inferred that the respondent sanctioned, approved or countenanced any of the primary acts of copyright infringement which have been found to have occurred.

777 I do not infer from the evidence that the respondent sanctioned or approved any such acts. I doubt that it is even open to me to do so in light of unchallenged findings of the primary judge. In my view, the appellants' case comes down to whether it can be inferred from the evidence that the respondent countenanced copyright infringement by iiNet users.

778 In *Jain* the Full Court found that Mr Jain had "countenanced" the acts of copyright infringement that occurred at licensed premises occupied by a company of which he was a director and chief executive officer. The Court (Sheppard, Foster and Hill JJ) said (26 FCR at 61):

> The 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 upon its own facts. Matters of degree are involved. But 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 it was likely that the appellant's music would be played without any licence from it. It was within his power to control what was occurring be he did nothing at all. In those circumstances we have reached the conclusion that the appellant established that Mr Jain authorised the infringement of copyright in question …"

779 As the primary judge pointed out, "countenance" is sometimes defined to mean to sanction or favour, or to patronize or encourage. As I have said, I do not think the respondent's conduct fits those descriptions. It is likely, however, that the Full Court in *Jain* had in mind some of the broader definitions of that word which can include "to tolerate" or "to permit". These words are useful synonyms so long as it is recognised that the word "authorise" itself connotes a mental element involving the giving of a consent or permission of some kind or a carelessness from which such consent or permission may be inferred.

780 In *Jain*, it was the respondent's decision to ignore the copyright owner's rights that was central to the Full Court's finding of authorisation. I do not think it is correct to say that the respondent in the present case ignored the appellants' rights. The respondent was of the view that it was not required to act on the AFACT notices because they were based upon allegations that required further investigation which the respondent did not believe it was required to undertake. I do not infer from this that it was in the respondent's mind to consent to or to permit copyright infringement by iiNet users using the respondent's facilities.

781 I accept that a refusal by an ISP to act on infringement allegations made by or on behalf of a copyright owner may be evidence from which authorisation might be inferred. But that will only be so if the refusal is unreasonable. Whether or not a refusal is unreasonable must depend upon the circumstances in which it occurs including the nature and quality of the information upon which the ISP is requested to act by the copyright owner.

782 Questions frequently arise in the area of copyright law upon which minds might reasonably differ, particularly when it comes to issues of originality, substantiality and fair dealing. Unintended consequences may follow if adverse inferences are too readily drawn against ISPs who refuse, in good faith, to act on infringement notices received from copyright owners. In particular, there is a danger that ISPs might be driven to act on infringement notices out of a desire to avoid involvement in potentially expensive and uncertain copyright litigation rather than any well founded acceptance of the substance of copyright owners' complaints.

783 My conclusion is that the respondent's failure to take steps to issue warning notices or to terminate or suspend subscribers' accounts in response to the allegations made in the AFACT notices was not unreasonable given the lack of information in the AFACT notices

which I have previously discussed. The fact that the respondent may not have acted on the AFACT notices even if they had contained additional information is beside the point. Nor does the fact that the respondent was provided with additional information during the course of the proceeding affect my conclusion given the circumstances in which this occurred.

Section 112E

784 Like the primary judge, I find it difficult to see how a person who merely did what s 112E describes could ever be found liable for authorisation even in the absence of that section. Nevertheless, in *Cooper* Branson J (with whom French J agreed) said (156 FCR at [39]):

> Additionally, … the introduction of s 112E into the Act suggests that, absent that section, a mere provider of facilities for making communications could have been held to have authorised copyright infringements effected by the use of those facilities. I do not accept, as Mr Cooper contended, that s 112E was introduced into the Act simply out of an abundance of caution. The supplementary explanatory memorandum for the *Copyright Amendment (Digital Agenda) Bill* 1999 (Cth) indicates otherwise by stating that the new 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.'

Those observations were not necessary to the decision in *Cooper*.

785 With great respect to their Honours, I doubt that it is correct to say that the presence of s 112E suggests that, in its absence, a person who merely provides facilities for making communications could be held to have authorised copyright infringement effected by the use of those facilities. Nor do I think the supplementary explanatory memorandum referred to by Branson J gives rise to any such suggestion.

786 Section 112E was introduced into the Act by the Digital Agenda Act. It was an object of that Act to "promote certainty for communication and information technology industries that are investing in and providing online access to copyright materials": s 3(b) Digital Agenda Act. It seems to me that s 112E puts beyond doubt what I think would have been reasonably clear in any event.

787 The primary judge referred to the legislative history of s 112E. His Honour noted (at [569]) that, contrary to observations made by Wilcox J in *Universal Music Australia Pty Ltd & Ors v Sharman License Holdings Ltd* (2005) 220 ALR 1 at [396]-[397], the legislative history suggested that s 112E was *not* to be understood as operating as a reversal of the High Court's decision in *Telstra*. Wilcox J's observations were picked up by Kenny J in *Cooper* at [168] where her Honour said:

> In order for s 112E to apply, there must be a person providing facilities "for making, or facilitating the making of, a communication". The appellants fall within this description. By force of s 112E, such a person is not to be taken to have authorised an infringement "merely because" another person uses the facilities in such a way as to infringe copyright. That is, if the most that can be said is that they have provided the facilities another person has used to infringe copyright, they are not to be taken to have authorised the infringement. As Wilcox J said in *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at [396], "[s]o understood, s 112E operates as a legislative reversal of the High Court's decision in *Telstra Corporation Limited v Australasian Performing Right Association Limited* (1997) 191 CLR 140". As his Honour noted at [399], 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 there are "other reasons" depends on the matters identified in s 101(1A) and any other relevant matters.

788 The High Court's decision in *Telstra* was not concerned with liability for authorisation. Rather, it was a case involving direct infringement under s 31(1)(iv) and (v) of Part III of the Act as it then stood. Since s 112E is by its terms concerned only with liability for authorisation, it is difficult to see how s 112E (or s 39B which is its Part III counterpart) could operate as a legislative reversal of the decision in *Telstra*.

789 The source of the confusion may be traced back to the Second Reading Speech for the *Copyright Amendment (Digital Agenda) Bill* 1999 (Hansard, 2 September 1999). The Attorney-General stated (at p 9750):

> The provisions in 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 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.

790 The amendments which were intended to overcome the decision in *Telstra* appear to be those made to s 22 of the Act. This is confirmed by the Advisory Report on the Copyright Amendment Act (Digital Agenda) Bill 1999 of the House of Representatives Standing

Committee on Legal and Constitutional Affairs (November 1999): see para 6.8 - 6.11 of the Advisory Report which expressly addresses the decision in *Telstra* in the context of proposed amendments to that section.

791 The enactment of s 39B and s 112E appears to have been prompted by the WIPO Copyright Treaty (December 1996). Article 8 provides that authors of literary and artistic works are to enjoy the exclusive right of authorising any communication to the public of their works. The agreed statement to Article 8 includes the following statement:

> It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention.

While it is inaccurate to speak of s 39B and s 112E as giving effect to the agreed statement, they are certainly in the spirit of it. The existence of the agreed statement at the time of the enactment of s 39B and s 112E tends to confirm, in my view, that both provisions were introduced out of an abundance of caution.

792 Difficulties can arise in relation to the interpretation of s 112E if it is approached as though it is there to protect a person from liability for authorisation which might otherwise arise under s 101(1). First, it can encourage an overly expansive interpretation of s 101(1) which is inconsistent with basic concepts established in *Moorhouse*. Secondly, it tends to give rise to a variety of complicated questions as to what a person must do, know or suspect before he or she is deprived of the protection of s 112E.

793 I can illustrate the latter point in this way. Clearly, a provider of communication facilities who actively encourages their use for the purpose of copyright infringement will have done something more than merely provide the communication facilities used to infringe copyright. The same is true of a person who not only makes the communication facilities available, but who also supplies the copyright material which is infringed through the use of those facilities. It is clear from the Full Court's decision in *Cooper* that s 112E would not apply to either of those situations.

794 However, the real problem arises in relation to knowledge. If a person makes communication facilities available knowing that they are to be used for the purpose of infringing copyright, can it be said that he or she has done something more than merely make

communication facilities available? The Full Court's decision in *Cooper* suggests so though in that case there was other conduct on the part of the ISP which contributed to the finding of authorisation made against the ISP. But what if the person makes communication facilities available not knowing, but merely suspecting, that they will at some stage be used in a manner that involves the infringement of copyright? That is likely to be true of most ISPs and many other persons in the business of providing communication facilities of various kinds. How is s 112E to operate in those circumstances assuming, of course, that the communication facilities made available by the ISP are later used in that manner?

795 There are no easy answers to these questions but they do not arise if s 112E is simply understood as making clear what I understand to be the true position under s 101(1) in any event, namely, it cannot be inferred that a person authorises copyright infringement merely because he or she provides another person with communication facilities used by the other person to infringe copyright.

796 Leaving aside the particular difficulties I have discussed, I agree with the analysis of s 112E adopted by the Full Court in *Cooper*.

797 If I had been satisfied that the respondent had approved, sanctioned or countenanced the acts of copyright infringement which have been found to have occurred, then I would have found the respondent liable for authorisation in spite of s 112E.

CONCLUSION ON AUTHORISATION

798 While I disagree with the primary judge's reasoning in significant respects, I am nevertheless of the opinion that his Honour's decision to dismiss the proceeding was correct. In my opinion the appeal should be dismissed. I agree with the order which Emmett J has proposed in relation to costs.

OTHER MATTERS

Telco Act

799 I agree with the reasons given by Jagot J for holding that that the AFACT notices, and the information which they contained, were not within the scope of s 276 of the Telco Act. I

also agree with her Honour that the respondent's customers consented to the disclosure and use of the score information and the rumba information for the purposes of administering and managing the services provided pursuant to the CRA and that the exception provided for in s 289 therefore applied to such information. To the extent that the respondent's services were used by persons who were not customers, I would infer that they also consented to the disclosure and use of the score information and the rumba information for such purposes. In the absence of evidence to the contrary, I think this may reasonably be inferred given that such persons elected to use a service which they may be taken to have known was made available upon terms. Accordingly, if it had been necessary for me to decide the question, I would have held that s 276 of the Telco Act did not prevent the respondent from using the AFACT information, the score information or the rumba information for the purpose of issuing warnings or terminating, suspending or restricting the supply of a service in accordance with relevant provisions of the CRA.

Safe Harbour Provisions

800 If I had come to the conclusion that the respondent was liable for authorisation, I would have held that it had not satisfied the conditions necessary to obtain the benefit of the limitations upon the relief which may be granted against the respondent specified in s 116AG(3).

801 It is common ground that the respondent is a carriage service provider which is relevantly engaged in Category A activity as defined by s 116AC of the Act.

802 Accordingly, in order to attract the benefit of s 116AG(3), the respondent need only comply with the conditions applicable to Category A activity as set out in the table incorporated in s 116AH(1), namely, Item 1 (Conditions 1 and 2) and Item 2 (Conditions 1 and 2). It is common ground that the respondent satisfies Conditions 1 and 2 of Item 2 and that Condition 2 of Item 1 does not apply. That leaves only Condition 1 of Item 1. It provides:

> The carriage service provider must adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers.

803 I have previously referred to the primary judge's finding that the respondent had a repeat infringer policy within the meaning of this condition. I disagree with that finding. I do not think the respondent had a repeat infringer policy and I think his Honour erred in holding that it did.

804 The condition which the respondent must satisfy requires the respondent to have adopted a policy "that provides for termination, in appropriate circumstances, of the accounts of repeat infringers." Nowhere in the Act or the Regulations are the expressions "repeat infringer" or "appropriate circumstances" defined. This may suggest that it was the legislature's intention that carriage service providers engaging in Category A activity should be given considerable latitude in determining who is a repeat infringer for the purposes of such a policy and in what circumstances the account of a repeat infringer should be terminated. Even so, the language used to describe the relevant condition must be given some work to do. There must be a policy providing for the termination of "repeat infringers". And the policy must provide for termination "in appropriate circumstances".

805 Turning to the first of these requirements, the policy which the primary judge found to exist is not a policy that has anything at all to say about repeat infringers. It does not even indicate who is a repeat infringer for the purposes of the policy. Rather, it is concerned with the termination of the accounts of people who have been found by a court or other authority to have engaged in copyright infringement or who have admitted to having engaged in copyright infringement. The respondent's policy, as found by the primary judge, provides that a subscriber will have his or her account terminated if found by a court or other authority to have infringed copyright even if he or she is found to have done so only once. This is not a policy which provides for the termination of the accounts of repeat infringers.

806 Nor do I accept that the respondent's policy provides for the termination of subscriber accounts in "appropriate circumstances". According to the respondent's policy, at least in the terms found by the primary judge, the respondent is not even required to terminate the accounts of subscribers who the respondent is satisfied have knowingly and repeatedly engaged in copyright infringement on a commercial scale. The respondent's policy provides for the termination of such an account only where such conduct has been the subject of an admission or a finding of a court or another authority. I do not see any rational basis for

finding that the respondent's policy is one that provides for termination in "appropriate circumstances" where it does not provide for termination in such a situation.

Leave to intervene

807 I agree with what Emmett J has said concerning the applications for leave to intervene.

I certify that the preceding two hundred and seventy-nine (279) numbered paragraphs are a true copy of the Reasons for Judgment herein of the Honourable Justice Nicholas.

Associate:

Dated: 24 February 2011

SCHEDULE I – THE APPELLANTS

UNIVERSAL CITY STUDIOS LLLP
Second Appellant

PARAMOUNT PICTURES CORPORATION
Third Appellant

WARNER BROS. ENTERTAINMENT INC
Fourth Appellant

DISNEY ENTERPRISES, INC
Fifth Appellant

COLUMBIA PICTURES INDUSTRIES, INC
Sixth Appellant

TWENTIETH CENTURY FOX FILM CORPORATION
Seventh Appellant

PARAMOUNT HOME ENTERTAINMENT (AUSTRALASIA) PTY LTD
(ACN 003 914 609)
Eighth Appellant

BUENA VISTA HOME ENTERTAINMENT, INC
Ninth Appellant

TWENTIETH CENTURY FOX FILM CORPORATION (AUSTRALIA) PTY LIMITED
(ACN 000 007 036)
Tenth Appellant

UNIVERSAL PICTURES (AUSTRALASIA) PTY LTD (ACN 087 513 620)

Eleventh Appellant

VILLAGE ROADSHOW FILMS (BVI) LTD

Twelfth Appellant

UNIVERSAL PICTURES INTERNATIONAL B.V.

Thirteenth Appellant

UNIVERSAL CITY STUDIOS PRODUCTIONS LLLP

Fourteenth Appellant

RINGERIKE GMBH & CO KG

Fifteenth Appellant

INTERNATIONALE FILMPRODUKTION BLACKBIRD VIERTE GMBH & CO KG

Sixteenth Appellant

MDBF ZWEITE FILMGESELLSCHAFT MBH & CO KG

Seventeenth Appellant

INTERNATIONALE FILMPRODUKTION RICHTER GMBH & CO KG

Eighteenth Appellant

NBC STUDIOS, INC

Nineteenth Appellant

DREAMWORKS FILMS L.L.C.

Twentieth Appellant

WARNER BROS INTERNATIONAL TELEVISION DISTRIBUTION INC

Twenty-First Appellant

TWENTIETH CENTURY FOX HOME ENTERTAINMENT INTERNATIONAL CORPORATION

Twenty-Second Appellant

WARNER HOME VIDEO PTY LTD (ACN 002 939 808)

Twenty-Third Appellant

PATALEX III PRODUCTIONS LIMITED

Twenty-Fourth Appellant

LONELY FILM PRODUCTIONS GMBH & CO KG

Twenty-Fifth Appellant

SONY PICTURES ANIMATION INC

Twenty-Sixth Appellant

UNIVERSAL STUDIOS INTERNATIONAL B.V.

Twenty-Seventh Appellant

SONY PICTURES HOME ENTERTAINMENT PTY LTD (ACN 002 489 554)

Twenty-Eighth Appellant

GH ONE LLC

Twenty-Ninth Appellant

GH THREE LLC

Thirtieth Appellant

BEVERLY BLVD LLC

Thirty-First Appellant

WARNER BROS ENTERTAINMENT AUSTRALIA PTY LTD
(ACN 003 773 411)

Thirty-Second Appellant

TWENTIETH CENTURY FOX HOME ENTERTAINMENT LLC

Thirty-Third Appellant

SEVEN NETWORK (OPERATIONS) LIMITED

(ACN 052 845 262)

Thirty-Fourth Appellant