

FEDERAL COURT OF AUSTRALIA

Roadshow Films Pty Ltd v Telstra Corporation Ltd [2016] FCA 1503

File numbers: NSD 239 of 2016
NSD 241 of 2016

Judges: **NICHOLAS J**

Date of judgment: 15 December 2016

Catchwords: **COPYRIGHT** – Section 115A of *Copyright Act 1968* (Cth) – where proceedings brought by copyright owners against carriage service providers (“CSPs”) providing internet access to customers – whether CSPs should be ordered to take reasonable steps to disable access to various online locations that infringe or facilitate the infringement of copyright – proper interpretation of s 115A(1) – appropriate form of injunctions and ancillary orders relating to existing and future scope and operation of injunctions – whether applicants should be required to pay CSPs’ costs of complying with injunctions and, if so, in what amounts – whether applicants should pay CSPs’ costs of the proceedings

Legislation: *Copyright Act 1968* (Cth) ss 10, 22, 86, 101, 115A, 116B(1)(a), 126, 132AC(1)(a), 132(1)(a)
Copyright Amendment (Online Infringement) Act 2015 (Cth)
Copyright Amendment (Online Infringement) Bill 2015
Federal Court of Australia Act 1976 (Cth) ss 23, 43
Telecommunications Act 1997 (Cth) ss 7, 16, 87
Children and Young Person Act 1969 (UK) s 1(2)

Cases cited: *Cooper v Universal Music Australia Pty Ltd* (2006) 156 FCR 380
In re D. (A Minor) [1987] 1 AC 317
Roadshow Films Pty Ltd v iiNet Ltd (2012) 248 CLR 42
Twentieth Century Fox Film & Ors v British Telecommunications plc [2011] EWHC 2714 (Ch)

Date of hearing: 23-24 June 2016

Date of last submissions: 22 November 2016

Registry: New South Wales

Division: General Division
National Practice Area: Intellectual Property
Sub-area: Copyright and Industrial Designs
Category: Catchwords

Number of paragraphs: 156

NSD 239 of 2016:

Counsel for the Applicants: Mr RPL Lancaster SC and Mr JS Cooke

Solicitor for the Applicants: Baker McKenzie

Counsel for the First to Third Respondents: Mr AJL Bannon SC and Mr AR Lang

Solicitor for the First to Third Respondents: King & Wood Mallesons

Counsel for the Fourth to Fifteenth Respondents: Mr JM Hennessy SC and Ms F St John

Solicitor for the Fourth to Fifteenth Respondents: Clayton Utz

Counsel for the Sixteenth to Twenty-Ninth Respondents: Mr BA Mee

Solicitor for the Sixteenth to Twenty-Ninth Respondents: Thomson Geer Lawyers

Counsel for the Thirty-Second and Thirty-Fourth to Fiftieth Respondents: Mr C Burgess

Solicitor for the Thirty-Second and Thirty-Fourth to Fiftieth Respondents: Aleco Vrisakis

NSD 241 of 2016:

Counsel for the Applicant: Mr RPL Lancaster SC and Ms JM Beaumont

Solicitor for the Applicant: Minter Ellison

Counsel for the First, Second and Eighteenth to Thirty-Third Respondents: Mr C Burgess

Solicitor for the First, Second and Eighteenth to Thirty-Third Respondents: Aleco Vrisakis

Counsel for the Third to Fourteenth Respondents: Mr JM Hennessy SC and Ms F St John

Solicitor for the Third to Fourteenth Respondents: Clayton Utz

Counsel for the Fifteenth to Seventeenth Respondents: Mr AJL Bannon SC and Mr AR Lang

Solicitor for the Fifteenth to Seventeenth Respondents: King & Wood Mallesons

Table of Corrections

21 December 2016	Para [90], third sentence be amended to read "... copyright in which is in some cases owned by Foxtel..."
21 December 2016	Para [111], first sentence be amended to read "...the facilitation of copyright infringement by the Torrentz sites..."
21 December 2016	Minor typographical corrections to paras [11], [14], [19], [22], [75], [88] and [153].

ORDERS

NSD 239 of 2016

BETWEEN: **ROADSHOW FILMS PTY LTD (ACN 100 746 870)**
First Applicant

VILLAGE ROADSHOW FILMS (BVI) LTD
(and others named in the Schedule)
Second Applicant

AND: **TELSTRA CORPORATION LTD (ACN 051 775 556)**
First Respondent

PACNET INTERNET (A) PTY LTD (ACN 085 213 690)
(and others named in the Schedule)
Second Respondent

JUDGE: **NICHOLAS J**

DATE OF ORDER: **15 DECEMBER 2016**

In these orders, the following terms have the following meanings:

- (a) **Domain Name** means a name formed by the rules and procedures of the **Domain Name System (DNS)** and includes subdomains.
- (b) **DNS Blocking** means a system by which any user of a respondent's service who attempts to use a DNS resolver that is operated by or on behalf of that respondent to access a Target Online Location is prevented from receiving a DNS response other than a redirection as referred to in order 5.
- (c) **IP Address** means an Internet Protocol address.
- (d) **Target Online Location** means:
 - (i) the online location or online locations known as "SolarMovie" that are or were accessible:
 - (A) at the following URLs:
 - (I) <https://www.solarmovie.is>
 - (II) <http://www.solarmovie.com>;
 - (III) <http://www.solarmovie.eu>; and
 - (IV) <https://www.solarmovie.ph>;

(together, the **Target URLs**);

(B) at the following IP Addresses:

(I) 185.47.10.11;

(II) 205.204.80.87;

(III) 188.92.78.142; and

(IV) 68.71.61.168;

(together, the **Target IP Addresses**);

(C) at the following Domain Names:

(I) solarmovie.is;

(II) solarmovie.com;

(III) solarmovie.eu; and

(IV) solarmovie.ph;

(together, the **Target Domain Names**).

- (e) **URL** means a Uniform Resource Locator;
- (f) **Telstra** means the first to third respondents;
- (g) **Optus** means the fourth to fifteenth respondents;
- (h) **M2** means the sixteenth to twenty-ninth respondents;
- (i) **TPG** means the thirty-second and the thirty-fourth to fiftieth respondents.

THE COURT ORDERS THAT:

1. The requirement under s 115A(4) of the *Copyright Act 1968* (Cth) that the applicants give notice of their application to the persons who operate the Target Online Location be dispensed with in so far as any such notice has not already been given.
2. Each respondent must, within 15 business days of these orders, take reasonable steps to disable access to the Target Online Location.
3. Order 2 is taken to have been complied with by a respondent if that respondent implements any one or more of the following steps:
 - (a) DNS Blocking in respect of the Target Domain Names;
 - (b) IP Address blocking or re-routing in respect of the Target IP Addresses;

- (c) URL blocking in respect of the Target URLs and the Target Domain Names;
or
 - (d) any alternative technical means for disabling access to a Target Online Location as agreed in writing between the applicants and a respondent.
4. If a respondent in complying with order 2 does not implement one of the steps referred to in order 3, that respondent must, within 15 business days of these orders, notify the applicants of the step or steps it has implemented.
5. Each respondent must redirect any communication by a user of its service seeking access to a Target Online Location which has been disabled pursuant to order 2 to a webpage established, maintained and hosted by either:
- (a) the applicants, or their nominee, pursuant to order 6; or
 - (b) that respondent or its nominee.

The applicants' obligations pursuant to orders 6 and 7 only arise if a respondent notifies the applicants that the respondent will redirect a communication pursuant to order 5(a) and for so long as at least one respondent redirects communications to that webpage.

6. The applicants, or their nominee, must establish, maintain and host a webpage which informs users of a respondent's service who have been redirected to the webpage pursuant to order 5 that access to the website has been disabled because this Court has determined that it infringes or facilitates the infringement of copyright.
7. Within 5 business days of these orders, the applicants will notify each of the respondents in writing of the URL of the webpage established, maintained and hosted under order 6 and, if the webpage ceases to operate for any reason, will notify each of the respondents in writing of a different URL that complies with order 6.
8. If, in complying with order 5, a respondent redirects any communication by a user of its service to a webpage established, maintained and hosted by it, that respondent or its nominee must ensure that the webpage informs the user of that respondent's service that access to that the website has been disabled because this Court has determined that it infringes or facilitates the infringement of copyright.
9. In the event that the applicants have a good faith belief that:

- (a) any Target URL, Target IP Address or Target Domain Name which is subject to these orders has permanently ceased to enable or facilitate access to a Target Online Location; or
- (b) any Target URL, Target IP Address or Target Domain Name has permanently ceased to have the primary purpose of infringing or facilitating the infringement of copyright,

a representative of the applicants must, within 15 business days of the applicants forming such a good faith belief, notify each respondent of that fact in writing, in which case the respondents shall no longer be required to take steps pursuant to order 2 to disable access to the relevant Target URL, Target IP Address or Target Domain Name that is the subject of the notice.

10. A respondent will not be in breach of order 2 if it temporarily declines or temporarily ceases to take the steps ordered in order 2 (either in whole or in part) upon forming the view, on reasonable grounds, that suspension is necessary to:

- (a) maintain the integrity of its network or systems, or functioning of its blocking system;
- (b) upgrade, troubleshoot or maintain its blocking system;
- (c) avert or respond to an imminent security threat to its network or system; or
- (d) ensure the reliable operation of its ability to block access to online locations associated with criminal content if it reasonably considers that such operation is likely to be impaired, or otherwise to comply with its statutory obligations including under section 313(3) of the *Telecommunications Act 1997* (Cth)

provided that:

- (e) unless precluded by law, it notifies the applicants or their legal representative(s) of such suspension, including the reasons and the expected duration of such suspension by 5.00 pm on the next business day; and
- (f) such suspension lasts no longer than is reasonably necessary and, in any case, no longer than 3 business days or such longer period as the applicants may agree in writing or the Court may allow.

11. The owner or operator of a Target Online Location and the owner or operator of any website who claims to be affected by these orders may apply on 3 days' written

notice, including notice to all parties, to vary or discharge these orders, with any such application to:

- (a) set out the orders sought by the owner or operator of the Target Online Location or affected website; and
- (b) be supported by evidence as to:
 - (i) the status of the owner or operator of the Target Online Location or affected website; and
 - (ii) the basis upon which the variation or discharge is sought.

12. The parties have liberty to apply on 3 days' written notice, including, without limitation, for the purpose of any application:

- (a) for further orders to give effect to the terms of these orders;
- (b) for further orders in the event of any material change of circumstances including, without limitation, in respect of the consequences for the parties and the effectiveness of the technical methods under order 2; and/or
- (c) for orders relating to other means of accessing a Target Online Location not already covered by these orders.

13. If the website the subject of a Target Online Location is at any time during the operation of these orders provided from a different Domain Name, IP Address or URL:

- (a) The applicants may file and serve;
 - (i) an affidavit which:
 - (A) identifies the different Domain Name, IP Address or URL;
 - (B) states that, in the good faith belief of the deponent, the website operated from the different Domain Name, IP Address or URL is a new location outside Australia for the Target Online Location the subject of these orders and brief reasons therefor; and
 - (ii) proposed short minutes of order to the effect that:

- (A) The definition of Target Online Locations in these orders is amended to include the different Domain Name, IP Address or URL; and
 - (B) The time period in order 2 of these orders starts to run in relation to the different Domain Name, IP Address or URL upon service in accordance with order 17(d) of the orders as made.
- 14. These orders are to operate for a period of 3 years from the date of these orders.
- 15. Six months prior to the expiry of these orders:
 - (a) the applicants may file and serve:
 - (i) an affidavit which states that, in the good faith belief of the deponent, a Target Online Location continues to have the primary purpose of infringing or facilitating the infringement of copyright; and
 - (ii) short minutes of order extending the operation of these orders for a further 3 year period; and
 - (b) the process contained in order 17 shall apply.
- 16. The affidavits referred to in orders 13 and 15 is to be given by a deponent duly authorised to give evidence on behalf of the applicants and may be given by their solicitor.
- 17. If an affidavit and short minutes of order are filed and served in accordance with orders 13 or 15:
 - (a) within 7 business days, the respondents must notify the applicants and the Court if they object to the orders being made in accordance with the short minutes of orders served by the applicants;
 - (b) if any respondent gives notice of any objection, or the Court otherwise thinks fit, the proceeding will be relisted for further directions;
 - (c) if no respondent gives notice of any objection and the Court does not otherwise require the proceeding to be relisted, then the Court may make orders in terms of the short minutes of orders served by the applicants without any further hearing; and

- (d) the applicants must serve on the respondents any such orders made.
18. The applicants pay Telstra's, Optus', M2's and TPG's compliance costs calculated at the rate of \$50 per Domain Name the subject of DNS Blocking undertaken for the purposes of complying with order 2 hereof.
 19. The applicants pay the respondents' costs as agreed or taxed of and incidental to the preparation of evidence and written submissions, and the making of oral submissions, in relation to the applicants' proposed order 12 and the issue of compliance costs (but excluding set-up costs referred to in [142] of the reasons for judgment).
 20. There be no other order as to costs.

Note: Entry of orders is dealt with in Rule 39.32 of the *Federal Court Rules 2011*.

ORDERS

NSD 241 of 2016

BETWEEN: **FOXTEL MANAGEMENT PTY LIMITED**
Applicant

AND: **TPG INTERNET PTY LTD (ACN 068 383 737)**
First Respondent

INET LIMITED (ACN 068 628 937)
(and others named in the Schedule)
Second Respondent

JUDGE: **NICHOLAS J**

DATE OF ORDER: **15 DECEMBER 2016**

In these orders, the following terms have the following meanings:

- (a) **Domain Name** means a name formed by the rules and procedures of the **Domain Name System (DNS)** and includes subdomains.
- (b) **DNS Blocking** means a system by which any user of a respondent's service who attempts to use a DNS resolver that is operated by or on behalf of that Respondent to access a Target Online Location is prevented from receiving a DNS response other than a redirection as referred to in order 5.
- (c) **IP Address** means an Internet Protocol address.
- (d) **Target Online Locations** means the online locations known as The Pirate Bay, Torrentz, TorrentHound and IsoHunt and that are or were accessible:
 - (A) at the URLs listed in the Schedule to this order (together, the **Target URLs**);
 - (B) at the IP Addresses listed in the Schedule to this order (together, the **Target IP Addresses**); and
 - (C) at the Domain Names listed in the Schedule to this order (together, the **Target Domain Names**).
- (e) **URL** means a Uniform Resource Locator.
- (f) **Telstra** means the fifteenth to seventeenth respondents;
- (g) **Optus** means the third to fourteenth respondents;

- (h) **TPG** means the first, second and eighteenth to thirty-third respondents.

THE COURT ORDERS THAT:

1. The requirement under s 115A(4) of the *Copyright Act 1968* (Cth) that the applicant give notice of its application to the persons who operate the Target Online Locations be dispensed with in so far as any such notice has not already been given.
2. Each respondent must, within 15 business days of these orders, take reasonable steps to disable access to the Target Online Locations.
3. Order 2 is taken to have been complied with by a respondent if that respondent implements any one or more of the following steps:
 - (a) DNS Blocking in respect of the Target Domain Names;
 - (b) IP Address blocking or re-routing in respect of the Target IP Addresses;
 - (c) URL blocking in respect of the Target URLs and the Target Domain Names;
or
 - (d) any alternative technical means for disabling access to the Target Online Locations as agreed in writing between the applicant and a respondent.
4. If a respondent in complying with order 2 does not implement one of the steps referred to in order 3, that respondent must, within 15 business days of these orders, notify the applicant of the step or steps it has implemented.
5. Each respondent must redirect any communication by a user of its service seeking access to a Target Online Location which has been disabled pursuant to order 2 to a webpage established, maintained and hosted by either:
 - (a) the applicant, or its nominee, pursuant to order 6; or
 - (b) that respondent or its nominee.

The applicant's obligations pursuant to orders 6 and 7 only arise if a respondent notifies the applicant that the respondent will redirect a communication pursuant to order 5(a) and for so long as at least one respondent redirects communications to that webpage.
6. The applicant, or its nominee, must establish, maintain and host a webpage which informs users of a respondent's service who have been redirected to the webpage

pursuant to order 5 that access to the website has been disabled because this Court has determined that it infringes or facilitates the infringement of copyright.

7. Within 5 business days of these orders, the applicant will notify each of the respondents in writing of the URL of the webpage established, maintained and hosted under order 6 and, if the webpage ceases to operate for any reason, will notify each of the respondents in writing of a different URL that complies with order 6.
8. If, in complying with order 5, a respondent redirects any communication by a user of its service to a webpage established, maintained and hosted by it, that respondent or its nominee must ensure that the webpage informs the user of that respondent's service that access to that the website has been disabled because this Court has determined that it infringes or facilitates the infringement of copyright.
9. In the event that the applicant has a good faith belief that:
 - (a) any Target URL, Target IP Address or Target Domain Name which is subject to these orders has permanently ceased to enable or facilitate access to a Target Online Location; or
 - (b) any Target URL, Target IP Address or Target Domain Name has permanently ceased to have the primary purpose of infringing or facilitating the infringement of copyright,a representative of the applicant must, within 15 business days of the applicant forming such a good faith belief, notify each respondent of that fact in writing, in which case the respondents shall no longer be required to take steps pursuant to order 2 to disable access to the relevant Target URL, Target IP Address or Target Domain Name that is the subject of the notice.
10. A respondent will not be in breach of order 2 if it temporarily declines or temporarily ceases to take the steps ordered in order 2 (either in whole or in part) upon forming the view, on reasonable grounds, that suspension is necessary to:
 - (a) maintain the integrity of its network or systems, or functioning of its blocking system;
 - (b) upgrade, troubleshoot or maintain its blocking system;
 - (c) avert or respond to an imminent security threat to its network or system; or

- (d) ensure the reliable operation of its ability to block access to online locations associated with criminal content if it reasonably considers that such operation is likely to be impaired, or otherwise to comply with its statutory obligations including under section 313(3) of the *Telecommunications Act 1997* (Cth)

provided that:

- (e) unless precluded by law, it notifies the applicant or their legal representative(s) of such suspension, including the reasons and the expected duration of such suspension by 5.00 pm on the next business day; and
- (f) such suspension lasts no longer than is reasonably necessary and, in any case, no longer than 3 business days or such longer period as the applicant may agree in writing or the Court may allow.

11. The owner or operator of any of the Target Online Locations and the owner or operator of any website who claims to be affected by these orders may apply on 3 days' written notice, including notice to all parties, to vary or discharge these orders, with any such application to:

- (a) set out the orders sought by the owner or operator of the Target Online Locations or affected website; and
- (b) be supported by evidence as to:
 - (i) the status of the owner or operator of the Target Online Locations or affected website; and
 - (ii) the basis upon which the variation or discharge is sought.

12. The parties have liberty to apply on 3 days' written notice, including, without limitation, for the purpose of any application:

- (a) for further orders to give effect to the terms of these orders;
- (b) for further orders in the event of any material change of circumstances including, without limitation, in respect of the consequences for the parties and effectiveness of the technical methods under order 2; and/or
- (c) for orders relating to other means of accessing the Target Online Locations not already covered by these orders.

13. If a website the subject of any of the Target Online Locations is at any time during the operation of these orders provided from a different Domain Name, IP Address or URL:

(a) the applicant may file and serve:

(i) an affidavit which:

(A) identifies the different Domain Name, IP Address or URL;

(B) states that, in the good faith belief of the deponent, the website operated from the different Domain Name, IP Address or URL is a new location outside Australia for the Target Online Locations the subject of these orders and brief reasons therefor; and

(ii) proposed short minutes of order to the effect that:

(A) the definition of Target Online Locations in these orders is amended to include the different Domain Name, IP Address or URL; and

(B) the time period in order 2 of these orders starts to run in relation to the different Domain Name, IP Address or URL upon service in accordance with order 17(d) of the orders as made.

14. These orders are to operate for a period of 3 years from the dates of these orders.

15. Six months prior to the expiry of these orders:

(a) the applicant may file and serve:

(i) an affidavit which states that, in the good faith belief of the deponent, that some or all of the Target Online Locations continue to have the primary purpose of infringing or facilitating the infringement of copyright; and

(ii) short minutes of order extending the operation of these orders in relation to the relevant Target Online Locations for a further 3 year period; and

(b) the process contained in order 17 shall apply.

16. The affidavits referred to in orders 13 and 15 are to be given by a deponent duly authorised to give evidence on behalf of the applicant and may be given by its solicitor.
17. If an affidavit and short minutes of order are filed and served in accordance with orders 13 or 15:
 - (a) within 7 business days, the respondents must notify the applicant and the Court if they object to the orders being made in accordance with the short minutes of orders served by the applicant;
 - (b) if any respondent gives notice of any objection, or the Court otherwise thinks fit, the proceeding will be relisted for further directions;
 - (c) if no respondent gives notice of any objection and the Court does not otherwise require the proceeding to be relisted, then the Court may make orders in terms of the short minutes of orders served by the applicant without any further hearing; and
 - (d) the applicant must serve on the respondents any such orders made.
18. The applicant pay Optus' compliance costs in the amount of \$1,500.
19. The applicant pay Telstra's and TPG's compliance costs calculated at the rate of \$50 per Domain Name the subject of DNS Blocking undertaken for the purposes of complying with order 2 hereof.
20. The applicant pay the respondents' costs as agreed or taxed of and incidental to the preparation of evidence and written submissions, and the making of oral submissions, in relation to the applicant's proposed order 12 and the issue of compliance costs (but excluding set-up costs referred to in [142] of the reasons for judgment).
21. There be no other order as to costs.

Note: Entry of orders is dealt with in Rule 39.32 of the *Federal Court Rules 2011*.

Schedule

A. The Pirate Bay

	Domain name	IP address	URL
1.	thepiratebay.se	141.101.118.194,141.101.118.195	https://thepiratebay.se/
2.	bayproxy.pw	104.27.167.96,104.27.166.96	https://bayproxy.pw/
3.	downloadbay.eu	104.28.1.53,104.28.0.53	http://downloadbay.eu/
4.	fastpiratebay.co.uk	104.27.174.252,104.27.175.252	https://fastpiratebay.co.uk/
5.	fastpiratebay.eu	104.28.26.119,104.28.27.119	https://fastpiratebay.eu/
6.	magnetsearch.org	104.24.122.173,104.24.123.173	https://magnetsearch.org/
7.	mypirateproxy.com	104.28.20.2,104.28.21.2	http://mypirateproxy.com/
8.	pirate.guru	104.28.17.148,104.28.16.148	https://pirate.guru/
9.	pirateahoy.eu	104.28.30.50,104.28.31.50	https://pirateahoy.eu/
10.	piratebay.host	198.41.249.68,162.159.240.69	https://piratebay.host/
11.	piratebaymirror.eu	104.28.2.19,104.28.3.19	https://piratebaymirror.eu/
12.	piratebayproxy.be	104.24.118.137,104.24.119.137	http://piratebayproxy.be/
13.	piratebays.co	104.27.168.249,104.27.169.249	https://piratebays.co/
14.	piratebays.co.uk	104.31.76.114,104.31.77.114	https://piratebays.co.uk/
15.	pirateproxy.ca	104.28.2.122,104.28.3.122	http://pirateproxy.ca/
16.	pirateproxy.tf	104.25.209.20,104.25.208.20	https://pirateproxy.tf/
17.	pirateproxy.wf	104.28.4.182,104.28.5.182	https://pirateproxy.wf/
18.	pirateproxy.yt	104.27.138.238,104.27.139.238	https://pirateproxy.yt/
19.	thebay.tv	104.28.6.185,104.28.7.185	https://thebay.tv/
20.	thepiratebay.casa	104.27.154.76,104.27.155.76	http://thepiratebay.casa/
21.	thepiratebay.cd	104.31.76.84,104.31.77.84	http://thepiratebay.cd/
22.	thepiratebay.cr	104.28.4.236,104.28.5.236	https://thepiratebay.cr/
23.	thepiratebay.expert	104.18.32.141,104.18.33.141	https://thepiratebay.expert/
24.	thepiratebay.org	104.18.40.167,104.18.41.167	http://thepiratebay.org/
25.	thepiratebay.uk.net	104.18.58.238,104.18.59.238	https://thepiratebay.uk.net/
26.	thepiratebay.xn--fiqs8s	104.28.2.96,104.28.3.96	http://thepiratebay.xn--fiqs8s/
27.	thepiratebay.xn--q9jyb4c	104.27.144.26,104.27.145.26	http://thepiratebay.xn--q9jyb4c/

	Domain name	IP address	URL
28.	thepiratebay-proxy.com	104.28.10.55,104.28.11.55	https://thepiratebay-proxy.com/
29.	thepirateboat.eu	104.28.6.62,104.28.7.62	https://thepirateboat.eu/
30.	tpbmirror.us	104.28.7.41,104.28.6.41	https://tpbmirror.us/
31.	urbanproxy.eu	104.28.13.69,104.28.12.69	https://urbanproxy.eu/

B. Torrentz

	Domain name	IP address	URL
1.	torrentz.eu	185.87.144.3,185.87.144.4,185.87.147.3,185.87.147.4	http://torrentz.eu/
2.	torrentsmirror.com	104.28.29.56,104.28.28.56	http://torrentsmirror.com/
3.	torrentz.ch	185.87.144.3,185.87.144.4,185.87.147.3,185.87.147.4	http://torrentz.ch/
4.	torrentz.com	72.52.4.119	http://torrentz.com/
5.	torrentz.hk	185.87.147.4,185.87.144.3,185.87.144.4,185.87.147.3	http://torrentz.hk/
6.	torrentz.in	185.87.147.3,185.87.147.4,185.87.144.3,185.87.144.4	http://torrentz.in/
7.	torrentz.li	185.87.147.4,185.87.144.3,185.87.144.4,185.87.147.3	http://torrentz.li/
8.	torrentz.me	185.87.144.3,185.87.144.4,185.87.147.3,185.87.147.4	http://torrentz.me/
9.	torrentz.ph	185.87.147.4,185.87.144.3,185.87.144.4,185.87.147.3	http://torrentz.ph/
10.	torrentz-proxy.com	185.87.144.3,185.87.144.4,185.87.147.3,185.87.147.4	http://torrentz-proxy.com/
11.	tz.ai	185.87.144.3,185.87.144.4,185.87.147.3,185.87.147.4	http://tz.ai/

C. TorrentHound

	Domain name	IP address	URL
1.	torrenthound.com	88.80.6.5	http://www.torrenthound.com/
2.	torrenthound.at	104.31.88.28, 104.31.89.28	http://torrenthound.at/
3.	torrenthound.cm	104.31.80.128, 104.31.81.128	http://torrenthound.cm/
4.	torrenthound.immunity.info	104.28.2.124, 104.28.3.124	https://torrenthound.immunity.info/
5.	torrenthound.ru	104.24.100.232, 104.24.101.232	http://torrenthound.ru/
6.	torrenthound.to	88.196.31.41	http://torrenthound.to/
7.	torrenthound.unlocktor.eu	5.45.77.184	http://torrenthound.unlocktor.eu/
8.	torrenthound-proxy.com	104.18.58.145, 104.18.59.145	http://torrenthound-proxy.com/

D. IsoHunt

	Domain name	IP address	URL
1.	isohunt.to	198.41.189.233, 198.41.190.233	https://isohunt.to/
2.	isohunt.duhsoft.com	5.45.75.223	http://isohunt.duhsoft.com/
3.	isohunt.kooaba.net	5.45.64.109	http://isohunt.kooaba.net/
4.	isohunt.st	173.236.194.74	http://www.isohunt.st/
5.	isohunters.net	78.142.19.12	http://isohunters.net/

REASONS FOR JUDGMENT

NICHOLAS J:

INTRODUCTION

- 1 These are my reasons for judgment in two proceedings that were heard together. In the first proceeding (“the Roadshow proceeding”) the applicants (“the Roadshow applicants”) seek relief under s 115A of the *Copyright Act 1968* (Cth) (“the Act”) against various carriage service providers (“CSPs”) requiring them to take reasonable steps to block access to a website. In the second proceeding (“the Foxtel proceeding”) the applicant (“Foxtel”) also seeks relief under s 115A against many of the same CSPs blocking access to various other websites. The applicants allege that the relevant websites are situated outside Australia and that they infringe, or facilitate the infringement of, copyright in large numbers of cinematograph films including motion pictures and television programs the copyright in which is owned by various applicants.
- 2 The respondents in each proceeding, and the corporate groups to which they belong, are as shown in the following table.

Group	Roadshow Proceeding	Foxtel Proceeding
Telstra	1 st to 3 rd respondents	15 th to 17 th respondents
Optus	4 th to 15 th respondents	3 rd to 14 th respondents
M2	16 th to 29 th respondents	-
TPG	32 nd and 34 th to 50 th respondents	1 st , 2 nd and 18 th to 33 rd respondents

The M2 respondents were not respondents in the Foxtel proceeding. All other respondents were party to both proceedings.

- 3 None of the operators of the relevant websites applied to be joined as a party to either proceeding and none sought to appear at the hearing or to make any submission. There was affidavit evidence in the proceedings given by solicitors acting for the applicants describing attempts to notify the persons who operate each of the relevant websites of the applications now before me. In light of that evidence I am satisfied that the applicants have made reasonable efforts to determine the identity and address of the persons who operate the

relevant websites, and to send notices to those persons. In circumstances where there has been no application by the persons who operate the relevant websites to be joined or any other acknowledgement by them indicating that they have been given notice of these applications, I propose to make orders pursuant to s 115A(4) of the Act dispensing with the requirement for the applicants to give those persons notice of the applications in so far as any such notice has not already been given.

4 There has been a large measure of co-operation between the applicants and the respondents. By the time of the hearing the parties were agreed upon a number of matters relating to the appropriate form of the orders that should be made in the event that the Court was satisfied that it should grant injunctive relief under s 115A of the Act. However, the respondents, who neither consented to nor opposed the grant of injunctive relief, only sought to be heard in relation to the form of orders and the terms upon which any relief under s 115A should be granted.

5 There was an order made in each proceeding that evidence in one be evidence in the other subject to any proper objections. The evidence was mostly given by way of affidavit with some brief oral evidence also given by Mr Carson, the applicant's expert witness in the Foxtel proceeding, and Mr Herps, the applicants' expert witness in the Roadshow proceeding. After the evidence was closed and submissions were completed, the applicants applied for leave to re-open to rely upon some additional affidavit evidence. None of the respondents opposed the applicants being given leave to re-open and, in the circumstances, I will grant the applicants the leave sought. In these reasons I refer to this additional evidence as the applicants' "supplementary evidence". The supplementary evidence was concerned with further inquiries made by the applicants after the close of the evidence in relation to some of the online locations the subject of their applications for orders under s 115A.

6 For reasons which I will explain I am satisfied that it is appropriate to grant an injunction under s 115A of the Act in each proceeding and to make various ancillary orders relating to its implementation.

TECHNICAL BACKGROUND

7 In this section of my reasons I provide some technical background relevant to the applications that are before me. This description of the technical background is substantially based upon evidence from the applicants' expert witnesses that was not contentious.

The Internet

- 8 The Internet is a network of interconnected computers and other digital devices. It enables computers or other digital devices (for convenience I will refer to all such devices as “computers”) to establish connections to other computers by cables or wireless technologies. These connections allow computers to communicate with other computers that are “online” using various protocols including the Internet protocol (“IP”) and transmission control protocol (“TCP”). A protocol in this context is a set of rules that computers use to communicate with one another. These communications are transmitted in packets of data sent or received by computers that are identified by their IP Addresses.

Internet Protocol Address

- 9 An Internet Protocol Address (“IP Address”) is a unique string of numbers separated by full stops that enables a computer to communicate with another computer via the Internet. A computer requires an IP Address to ensure that data sent over the Internet reaches its intended destination. Internet Service Providers (“ISPs”) usually provide their customers with access to the Internet via a router to which the ISP assigns an IP Address. Blocks of IP Addresses are allocated by the Internet Assigned Numbers Authority (“IANA”) to five Regional Internet Registries (“RIR”) which then allocate them to ISPs and other entities.

Uniform Resource Locator

- 10 A Uniform Resource Locator (“URL”) is a reference (an address) to a resource, such as a computer server, an electronic document, or a webpage on the Internet, and refers to the entire address used to fetch a resource from an online location. A URL has two main components, a Protocol Identifier and a Resource Name. The Protocol Identifier indicates the name of the Protocol to be used to fetch the resource. For example “https” is the Protocol Identifier which tells a computer to use a protocol known as a Hyper Text Transfer Protocol Secure (“HTTPS”). HTTPS is a secure version of Hyper Text Transfer Protocol (“HTTP”). Both protocols can be used to send data between an online computer and another online location such as a website. The Resource Name refers to the computer that contains the relevant resource, such as a webpage, together with other information (eg. directory, subdirectory and file name) that may be required to locate and access the resource on that computer.

Domain Names

- 11 The Domain Name System (“DNS”) is the system for naming computer servers and other resources connected to the Internet. A Domain Name is a complete address to a resource on the Internet. Domain Names are allocated by a Domain Name Registrar. While the Internet works with IP Addresses, Domain Names provide a more user friendly way for users to interact with the Internet. A computer’s web browser works in the background to seamlessly translate typed Domain Names (eg. “google.com”) into an IP Address (eg. 74.125.224.72). A DNS query is a process whereby a computer or networking device makes an inquiry with a DNS server to find a server that contains the IP Address for the Domain Name. The label at the end of a Domain Name (eg. “.com”) is the top level domain (“TLD”). The core group of TLDs are maintained by IANA and are “com”, “info”, “net” and “org”. There are also many different country code TLDs (“ccTLDs”). IANA is responsible for delegating the management of these ccTLDs (eg. .au, .us, and .uk) to a trustee which is often required to have a local presence in the relevant country.

Domain Name System Server

- 12 A Domain Name System server (also known as a “DNS server”, a “DNS resolver” or simply “DNSS”) is a server connected to the Internet that manages, maintains and processes compilations of Domain Names and other related information. A DNSS translates (or resolves) a Domain Name into an IP address. The DNSS that is assigned by the holder of a Domain Name to manage domain name lookups is an “authoritative DNSS”. DNS resolution is usually performed by an ISP (using its own DNSS) as part of its service to customers.

DNS Blocking

- 13 Usually, a user’s computer will contact the DNSS operated by the user’s ISP whenever the user’s computer needs to resolve a Domain Name to an IP Address. In normal operation, the DNSS will return the IP Address authoritatively specified by the holder of the Domain Name. However, ISPs can block access to specific online locations entered into the address bar of the Internet browser, by configuring their DNSS to either return no IP Address so that an error message is displayed to users or so that users are directed to a predetermined IP Address that differs from that designated by the specific online location’s IP Address. This is known as DNS blocking.

URL Blocking

- 14 URL blocking works by performing a process known as “packet inspection”. A “packet” is a piece of data routed between an origin and a destination on the Internet. URL blocking requires ISPs to maintain a list of URLs that are to be blocked which may then be compared against the destinations specified in packets sent across the ISP’s network. If the URL for a given destination is blocked, traffic will not be sent to that destination. URL Blocking does not work for secure Internet traffic (eg. using the “https” protocol) unless deep packet inspection technology is used because the packets transmitted are encrypted and cannot be inspected.

IP Address Blocking

- 15 IP Address blocking prevents the connection between a server or website and certain IP Addresses. IP Address blocking is achieved by the ISP not routing the outbound traffic to the IP Addresses of specific online locations. IP Address blocking can be problematic as an IP Address associated with a website may also be associated with different unrelated websites that are also hosted on the same server. In particular, website hosting providers may store the content for many different websites on one host server which may share one or more IP Addresses.

Proxy Servers

- 16 Proxy servers are intermediary computers that relay data between a sender and receiver though they may sometimes do more than this. They can be used to speed up performance by caching data that may be more quickly and reliably accessed via a proxy server than from the originating or principal server. A proxy server often encapsulates packets passing through with its own IP Address to give the appearance that it is the originating server.

BitTorrent

The BitTorrent Protocol

- 17 BitTorrent is a protocol designed for the efficient and decentralised sharing of electronically stored information across the Internet. BitTorrent is particularly useful for sharing large files and is therefore well suited for the sharing of music, movies and television programs. BitTorrent is known as a peer to peer (“P2P”) protocol as all peers downloading data will, by design, immediately begin sharing that data with other peers by making data available online

to other BitTorrent users. The sharing of electronic information using BitTorrent requires a number of essential components described further below.

BitTorrent clients

- 18 A BitTorrent client is a computer program that allows users to identify, download and share data. A BitTorrent client communicates with other BitTorrent clients using the BitTorrent protocol. There are several well-known BitTorrent clients. A popular BitTorrent client is called uTorrent (“uTorrent”) which is user friendly and freely available for use on all popular operating systems.

piece/torrent files / magnet links

- 19 BitTorrent breaks the data that is to be shared (whether a single file or a collection of many files) into “pieces” that together make up a “Payload”. The Payload can then be distributed across the Internet in pieces before reassembly by a BitTorrent client. Torrent files are small files that instruct the BitTorrent client where to find a Payload consisting of data from which a copy of an entire film or sound recording can be assembled. A torrent file does not contain any of the data but does include other information relevant to file sharing operations (known as metadata) including:

- the web address or URL of the tracker (described below);
- the filename;
- the size of each piece the file is broken into;
- the cryptographic code (hash value) of each file piece;
- the hash value of the whole file.

- 20 Groups of computers sharing the same torrent file are known as a “swarm”. Each computer in a swarm is known as a “peer”. A peer that has a complete copy of the Payload is known as a “seed”. A “magnet link” in simple terms is a hyperlink to an associated torrent file which may be used to trigger the downloading of data from other peers.

Trackers

- 21 A tracker is a BitTorrent based computer program (“Tracker”) running on an Internet connected computer. Magnet links usually include information about the location of one or more Trackers. Using that information BitTorrent clients will attempt to connect with the Tracker in order to access the swarm from which they will obtain the Payload. There may be

several Trackers specified in a magnet link but only one active Tracker is required to gain access to a Payload. A Tracker will provide BitTorrent clients with a directory of peers who are making data available and peers who are seeking data together with details of their IP Addresses. It will provide to a BitTorrent client requesting a specific Payload details of the IP Addresses of peers from which the Payload may be obtained.

CloudFlare/MaxMind/Whois

22 CloudFlare Inc (“CloudFlare”) provides an online service that acts as an intermediary for websites. CloudFlare is known as a “reverse proxy” because it retrieves information on behalf of its customer’s servers and returns this information as though it originated from a CloudFlare server. Users of CloudFlare allow the service to act as the authoritative DNS for their websites and it will often allocate two or more IP Addresses to them. CloudFlare offers its users:

- (a) a large network of worldwide servers to provide efficient traffic delivery to their website using CloudFlare owned IP Addresses;
- (b) no direct connection to customer IP Addresses reducing the risk of being hacked or denial of service attacks;
- (c) caching of key components of a website reducing the amount of traffic required to be delivered to a given website and speeding up responses back to user requests; and
- (d) an “always online” service for when the customer’s website is down for maintenance during which period, CloudFlare will present cached copies of webpages.

23 It is clear that at least some of these services will appeal to a person operating a website engaged in illicit activities (including copyright infringement or the facilitation of copyright infringement) who may wish to conceal the details of any IP Addresses used by his or her computer.

24 “MaxMind” is one of a number of online services that can be used to ascertain the country code, geographical location, postal code, geographic coordinates associated with an IP Address and the name of the ISP (or other entity) to which an IP Address has been allocated. “Whois” is an online service which provides information relating to the ownership of Domain Names.

RELEVANT STATUTORY PROVISIONS

Section 115A

25 Section 115A was introduced into the Act by the *Copyright Amendment (Online Infringement) Act 2015* (Cth) (“the Amendment Act”) with effect from 27 June 2015. The Copyright Amendment (Online Infringement) Bill 2015 was first introduced into the House of Representatives where it was amended before it came to be considered by the Senate. The explanatory memorandum tabled in the House of Representatives was revised to take account of those amendments. A revised explanatory memorandum to the Copyright Amendment (Online Infringement) Bill 2015 (“the Revised Explanatory Memorandum”) was tabled in the Senate.

26 Section 115A, which is in Part V, Div 2 of the Act, provides:

115A Injunctions against carriage service providers providing access to online locations outside Australia

- (1) The Federal Court of Australia may, on application by the owner of a copyright, grant an injunction referred to in subsection (2) if the Court is satisfied that:
 - (a) a carriage service provider provides access to an online location outside Australia; and
 - (b) the online location infringes, or facilitates an infringement of, the copyright; and
 - (c) the primary purpose of the online location is to infringe, or to facilitate the infringement of, copyright (whether or not in Australia).
- (2) The injunction is to require the carriage service provider to take reasonable steps to disable access to the online location.

Parties

- (3) The parties to an action under subsection (1) are:
 - (a) the owner of the copyright; and
 - (b) the carriage service provider; and
 - (c) the person who operates the online location if, but only if, that person makes an application to be joined as a party to the proceedings.

Service

- (4) The owner of the copyright must notify:
 - (a) the carriage service provider; and
 - (b) the person who operates the online location;of the making of an application under subsection (1), but the Court may

dispense, on such terms as it sees fit, with the notice required to be sent under paragraph (b) if the Court is satisfied that the owner of the copyright is unable, despite reasonable efforts, to determine the identity or address of the person who operates the online location, or to send notices to that person.

Matters to be taken into account

- (5) In determining whether to grant the injunction, the Court may take the following matters into account:
- (a) the flagrancy of the infringement, or the flagrancy of the facilitation of the infringement, as referred to in paragraph (1)(c);
 - (b) whether the online location makes available or contains directories, indexes or categories of the means to infringe, or facilitate an infringement of, copyright;
 - (c) whether the owner or operator of the online location demonstrates a disregard for copyright generally;
 - (d) whether access to the online location has been disabled by orders from any court of another country or territory on the ground of or related to copyright infringement;
 - (e) whether disabling access to the online location is a proportionate response in the circumstances;
 - (f) the impact on any person, or class of persons, likely to be affected by the grant of the injunction;
 - (g) whether it is in the public interest to disable access to the online location;
 - (h) whether the owner of the copyright complied with subsection (4);
 - (i) any other remedies available under this Act;
 - (j) any other matter prescribed by the regulations;
 - (k) any other relevant matter.

Affidavit evidence

- (6) For the purposes of the proceedings, section 134A (affidavit evidence) applies as if the reference in paragraph 134A(f) to a particular act included a reference to a class of acts.

Rescinding and varying injunctions

- (7) The Court may:
- (a) limit the duration of; or
 - (b) upon application, rescind or vary;
- an injunction granted under this section.
- (8) An application under subsection (7) may be made by:
- (a) any of the persons referred to in subsection (3); or

- (b) any other person prescribed by the regulations.

Costs

- (9) The carriage service provider is not liable for any costs in relation to the proceedings unless the provider enters an appearance and takes part in the proceedings.

27 The term “online location” is not defined in the Act. According to the Revised Explanatory Memorandum (at [36]):

The term ‘online location’ is intentionally broad and includes, but is not limited to, a website, and would also accommodate future technologies.

28 The Revised Explanatory Memorandum also includes the following observations concerning the purpose of s 115A which is to reduce online copyright infringement:

1. The purpose of this Bill is to introduce a key reform to reduce online copyright infringement. The scheme is deliberately prescriptive; it is intended as a precise response to a specific concern raised by copyright owners.
2. The Bill amends the *Copyright Act 1968* (the Act) to enable the owner of a copyright to apply to the Federal Court of Australia for an order requiring a Carriage Service Provider (CSP) to block access to an online location that has the primary purpose of infringing copyright or facilitating the infringement of copyright.
3. The Bill provides that copyright owners would be able to apply directly to the Federal Court for an injunction to disable access to an infringing online location, without having to first establish the CSP’s liability for copyright infringement or authorisation of copyright infringement. This judicial process would be more efficient and avoid implicating CSPs unnecessarily.

29 The Revised Explanatory Memorandum also states at [6]-[7]:

6. The factors that the Court may take into account set an intentionally high threshold test for satisfaction by the Court. The purpose of the scheme is to allow a specific and targeted remedy to prevent those online locations which flagrantly disregard the rights of copyright owners from facilitating access to infringing copyright content.
7. The Bill contains a standalone injunction power which operates as a no-fault remedy. It would not affect existing laws on infringement, copyright exceptions or limitations, authorisation liability or any of the safe harbour conditions. Further, the Court granting an injunction would not create a presumption that the CSP has infringed copyright nor authorised the infringement of copyright.

30 It is important to note that s 115A provides for a “no fault” remedy against a CSP. In particular, the entitlement of an applicant for relief under s 115A does not depend upon it

establishing that the CSP against which it seeks such relief has committed an infringement of copyright either by its own acts or by authorising the acts of another person.

31 If the applicant satisfies the Court that the CSP provides access to an online location outside Australia, that the primary purpose of the online location is to infringe, or facilitate the infringement of copyright, and that the online location infringes or facilitates the infringement of the applicant's copyright, then the conditions necessary to permit the Court to grant an injunction will be fulfilled.

32 It is not necessary for the applicant to establish any element of knowledge or intention on the part of a CSP for the applicant to obtain relief against it under s 115A. Although the CSP's knowledge might be relevant to the exercise of the Court's discretion in a particular case, the scheme of s 115A, as the Revised Explanatory Memorandum makes clear, is designed to avoid the kind of factual inquiries into matters of the kind undertaken in a proceeding taken against a CSP for copyright infringement based upon "authorisation": see *Roadshow Films Pty Ltd v iiNet Ltd* (2012) 248 CLR 42; *Cooper v Universal Music Australia Pty Ltd* (2006) 156 FCR 380.

33 The relief that may be granted under s 115A consists of an injunction against a CSP requiring it "to take reasonable steps to disable access to the online location." This is the sole relief provided for in s 115A(2) although it is also open to the Court to grant its injunction conditionally or by the imposition of terms requiring the applicant, for example, to indemnify (in whole or part) a CSP against whom the injunction is sought, or to provide security for a CSP's costs of complying with an injunction granted pursuant to s 115A. The Revised Explanatory Memorandum gives an example (at [42]) of an order requiring that an appropriate indemnity or undertaking be provided by a party who obtains an injunction under s 115A(2) of the Act.

34 There are also other statutory provisions found in the *Federal Court of Australia Act 1976* (Cth) ("the Federal Court Act") that enable ancillary orders to be made including, generally, s 23 and, specifically with respect to costs, s 43. Section 23 of the Federal Court Act would enable the Court in a proceeding brought under s 115A to make other orders ancillary or incidental to any injunctive relief granted under that section. Section 43 of the Federal Court Act also confers on the Court power to award costs in all proceedings before the Court subject to some exceptions that are not relevant to proceedings under s 115A of the Act. However, s 43 must be read subject to s 115A(9) of the Act which provides, in substance, that

a CSP is not liable for any costs in a proceeding under s 115A unless it enters an appearance and takes part in the proceeding.

Specific requirements of Section 115A(1)

35 It is now necessary to refer in more detail to the specific requirements of s 115A(1). The first point to note is that the language of the chapeau makes clear that the Court may only grant the relevant injunctive relief if it is satisfied as to the existence of the matters referred to in s 115A(1) subsections (a), (b) and (c) which I shall refer to as “the s 115A(1) requirements”. Whether the Court proceeds to grant an injunction, in circumstances where the s 115A(1) requirements are satisfied, will depend on whether it determines that it is appropriate to do so in the circumstances of the particular case.

Section 115A(1)(a) – “a carriage service provider provides access to an online location outside Australia”

36 Section 10 of the Act provides that “carriage service provider” has the same meaning as in the *Telecommunications Act 1997* (Cth) (“the Telco Act”). Section 87(1) of the Telco Act states:

87 Carriage service providers

Basic definition

- (1) For the purposes of this Act, if a person supplies, or proposes to supply, a listed carriage service to the public using:
- (a) a network unit owned by one or more carriers; or
 - (b) a network unit in relation to which a nominated carrier declaration is in force;
- the person is a carriage service provider.

37 Section 7 of the Telco Act provides that carriage service means “a service for carrying communications by guided and/or unguided electromagnetic energy.” A “listed carriage service” is defined in s 16(1) of the Telco Act to include a carriage service between a point in Australia and one or more points in Australia. It was not disputed that each of the respondents is a CSP as defined in s 87(1) of the Telco Act.

38 The requirement in s 115A(1)(a) that a CSP provides access to “an online location outside Australia” constitutes an important limitation on the power of the Court to make an order under s 115A(2). This limitation may reflect an assumption that other provisions of the Act provide copyright owners with adequate remedies in respect of online locations situated

within Australia that have, as their primary purpose, copyright infringement or the facilitation of copyright infringement.

39 Exactly the same electronic information (eg. webpage content) may be made available from more than one online location. It therefore cannot be assumed that because the information available from a number of different Domain Names, URLs or IP Addresses appears to be, or is, exactly the same, that the information is necessarily made available from the same online location.

40 This is a matter of some importance given the requirements of s 115A(1) which, by implication at least, may limit the availability of relief under s 115A(1) to situations in which (inter alia) the online location is situated outside Australia. At first glance, s 115A appears not to enable an order to be made requiring a CSP to disable access to a proxy server located in Australia even though it is a mere conduit for communications between another online location situated outside Australia and Internet users in Australia. Whether s 115A could be invoked in respect of a proxy server in such circumstances may depend, perhaps, upon whether it could be said that the CSP provides access to the primary server notwithstanding the interposition of the proxy server. It is not necessary to decide this question in the present proceedings because I am satisfied that the proxy servers referred to in the evidence are all situated outside Australia.

41 There is also a question which I need to address arising out of the use of the present tense (“provides access”) in s 115A(1)(a). A similar question arises with respect to s 115A(1)(b) which is also expressed in the present tense (“infringes or facilitates”). I will return to this topic shortly.

Section 115A(1)(b) “the online location infringes, or facilitates an infringement of, the copyright”

42 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.

43 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 ...

44 Section 22(6)-(6A) of the Act 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.

45 Section 101 relates to the infringement of copyright in subject-matter other than works, which includes cinematograph films and sound recordings. Section 101(1) provides that, subject to the Act, copyright 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 authorises the doing in Australia of, any act comprised in the copyright. Section 101(1A) includes a list of factors that must be taken into account in determining whether or not a person has “authorised the doing” of a relevant act.

46 It is apparent from these provisions that acts of infringement are acts of persons. An inanimate object or an online location (such as a website) cannot itself infringe copyright under s 101(1) though it may facilitate an infringement of copyright. To the extent s 115A(1)(b) refers to an online location that “infringes copyright” it may be understood as referring to acts comprised within the copyright as defined, in the case of cinematograph films, in s 86 of the Act. Thus, an online location will infringe copyright in a cinematograph film in the sense described in s 115A(1)(b) if the online location performs any of the acts referred to in s 86 without the licence of the copyright owner. These include the act of making available online, or electronically transmitting, a copy of the film. It necessarily follows that s 115A(1) permits the grant of an injunction in circumstances where it is

impossible to say who is responsible for operating the online location or determining the content of any material made available online at the online location.

- 47 Even if the online location does not itself infringe copyright, the requirements of s 115A(1)(b) may be satisfied if the online location “facilitates” an infringement of copyright. The language used is deliberately broad. The word “facilitate” means “to make easier or less difficult; help forward (an action or process etc)”: *Macquarie Dictionary* (6th ed, 2013) at 525. In determining whether an online location facilitates the infringement of copyright, the Court will seek to identify a species of infringing act and ask whether the online location facilitates that act by making its performance easier or less difficult. An online location may both infringe and facilitate the infringement of copyright by making an electronic copy of a work or other subject matter available online for transmission to users. But it may also facilitate the infringement of copyright merely by making it easier for users to ascertain the existence or whereabouts of other online locations that themselves infringe or facilitate the infringement of copyright.

Section 115A(1)(c) – the “primary purpose of the online location is to infringe, or to facilitate the infringement of, copyright (whether or not in Australia)”

- 48 The requirement that the online location have as its primary purpose copyright infringement or the facilitation of copyright infringement provides an important check on the operation of s 115A. Thus, the fact that a particular website makes some unlicensed copyright material available online or is routinely used by some users to infringe copyright does not establish that the primary purpose of the website is to infringe or facilitate the infringement of copyright. The s 115A(1)(c) requirement is explained in the Revised Explanatory Memorandum as follows:

38. The Court must also be satisfied that the primary purpose of the online location is to either infringe copyright, or facilitate the infringement of copyright generally. This is an intentionally high threshold for the copyright owner to meet as a safeguard against any potential abuse. For example, the ‘primary purpose’ test would prevent an injunction to disable access to an art gallery website operated outside of Australia that may contain an unauthorised photograph. Thus, a website such as www.youtube.com or www.blogger.com would not prima facie satisfy the test as being an online location that infringes or facilitates infringement of copyright. Technology and technological change is not to be chilled or targeted by this amendment.
39. The primary purpose test would also prevent an injunction to block an online location operated overseas that provides legitimate copyright material to individuals within another geographic location, but are not licensed to distribute that copyright material in Australia. For example, the United

States iTunes store does not operate with the primary purpose of infringing copyright or facilitating the infringement of copyright and therefore access to this online location would not be disabled under an injunction. The test is also not intended to capture Virtual Private Networks (VPNs) that are promoted and used for legitimate purposes, or merely used to access legitimate copyright material distributed in a foreign geographic market. VPNs have a wide range of legitimate purposes and have no oversight, influence or control over their customers' activities.

40. ***The primary purpose test would direct the Court to consider the principal activity for which the online location exists and the principal intention of users of that online location.*** Purpose may be distinct from motive. An online location may have the 'primary purpose' of infringing, or facilitating the infringement of copyright even if the operator of the location derives a commercial advantage or profit from the operation of the location. For example, where an online location has copyright infringement as the principal activity for which it exists and the principal reason for attracting visits to the online location, the fact that the motive or incentive of its operator is to draw profits from advertising revenue does not mean that its primary purpose is to profit from advertising rather than to infringe copyright.

(Emphasis added)

- 49 The purpose of the online location may be ascertained by a consideration of the use that is or may be made of it. If the Court is satisfied that the principal activity for which the online location is used or designed to be used is copyright infringement or the facilitation of copyright infringement, then it will be open to conclude that the primary purpose of the online location is to infringe, or to facilitate the infringement of, copyright.

Temporal Issues

- 50 The supplementary evidence raises an issue in relation to the time at which the Court must be satisfied of the matters referred to in s 115A(1) of the Act. There are three obvious possibilities: (1) the date of commencement of the proceeding; (2) the date of the hearing and (3) the time of granting the injunction. In my opinion the Court must be satisfied of the various matters referred to in s 115A(1) of the Act at the time of granting the injunction. If the Court was, at the time of giving consideration to the making of an order under s 115A(1), not so satisfied, then it should not grant the injunction.
- 51 Some statutory provisions, expressed in what is sometimes referred to as the continuous present, have been construed so as to require the existence of a continuum. For example, s 1(2) of the *Children and Young Person Act 1969* (UK) provided that the juvenile court could make a care order if it was of the opinion that any one of three conditions were satisfied including that a child's "health is being avoidably impaired or neglected ..." (emphasis

added). The meaning of this provision was considered by the House of Lords in *In re D. (A Minor)* [1987] 1 AC 317. Lord Goff said at 350:

The words “is being” are in the continuous present. So there has to be a continuum in existence at the relevant time [...]. In cases under the subsection, this may not be established by proof of events actually happening at the relevant time. In the nature of things, it may well have to be established, as continuing at that time, by evidence that (1) the relevant state of affairs had existed in the past, and (2) there is a likelihood that it will continue into the future.

52 However, in my view, the words “provides”, “infringes” and “facilitates” as they appear in s 115A(1)(a) and (b) are neutral in temporal meaning in that they may apply to past as well as to present conduct. Part V of the Act contains other instances of such usage: see, for example, s 116B(1)(a) (“a person receives”), s 132AC(1)(a) (“engages in conduct”), s 132(1)(a) (“makes an article”).

53 As previously mentioned, the term “online location” is not defined. In my view it can include a location, such as a website, that was online at the time the relevant proceeding was commenced but is not online either at the time of the hearing or at the time of granting the injunction. The Revised Explanatory Memorandum recognises that s 115A is “deliberately prescriptive” and that it provides a “precise response to a specific concern raised by copyright owners.” However, when interpreting s 115A it is necessary to consider the purpose of the provision, which is to provide an efficient means of blocking access to online locations operated outside Australia that have as their primary purpose the infringement, or the facilitation of the infringement, of copyright. Too narrow a reading of the language used in s 115A(1) would deprive the section of much of its usefulness eg. if it were construed so as to allow an operator to avoid an injunction simply by taking a website off-line temporarily for a period of days, weeks or months during the course of the relevant proceeding.

54 For all these reasons I do not consider that s 115A(1) requires that the Court be satisfied, at the time of granting an injunction, that the respondent CSP is providing access to the online location at that moment in time or that the online location is, at the moment of granting the injunction, infringing or facilitating the infringement of copyright. Of course, the fact that the online location is not online or has been otherwise disabled by the time of the hearing, or at any other time at which consideration is given to the making of an order s 115A(1), may be a matter relevant to the exercise of the Court’s discretion.

Section 126

55 The applicants in both proceedings relied upon s 126 of the Act in relation to the proof of subsistence and ownership of copyright in cinematograph films being either motion pictures or television programs in which they claimed to own copyright. Section 126, which is in Part V, Div 4 of the Act, provides:

126 Presumptions as to subsistence and ownership of copyright

In an action brought by virtue of this Part:

- (a) copyright shall be presumed to subsist in the work or other subject-matter to which the action relates if the defendant does not put in issue the question whether copyright subsists in the work or other subject-matter; and
- (b) where the subsistence of the copyright is established—the plaintiff shall be presumed to be the owner of the copyright if he or she claims to be the owner of the copyright and the defendant does not put in issue the question of his or her ownership.

56 Part V, Div 4 of the Act also includes various other provisions creating presumptions that may apply where the defendant puts in issue the question of subsistence or ownership of copyright.

THE ROADSHOW PROCEEDING

The Roadshow films

57 The second to eighth applicants in the Roadshow proceeding claim to be the owners of copyright in the following motion pictures and television programs (“the Roadshow films”):

Title	Copyright Owner
The Lego Movie	Second applicant
Tron Legacy	Third applicant
Cinderella	Third applicant
Spy	Fourth applicant
Kingsman: The Secret Service	Fourth applicant
Transformers: Age of Extinction	Fifth applicant
The Gambler	Fifth applicant
Spider-Man 2	Sixth applicant
This Is The End	Sixth applicant
Jurassic World	Seventh applicant
Straight Outta Compton	Seventh applicant
The Big Bang Theory: Season 7, Episode 24	Eighth applicant
Shameless: Season 4, Episode 12	Eighth applicant

- 58 None of the respondents put either subsistence or ownership of copyright in issue in the Roadshow proceeding nor did any suggest that it was not open to the applicants to rely upon s 126 in a proceeding under s 115A. In my view it is open to the Roadshow applicants to rely upon s 126 in this case. In the absence of any evidence to suggest that the second to eighth Roadshow applicants are not the owners of copyright in the Roadshow films then subsistence and ownership should be taken to be established.

SolarMovie

- 59 The Roadshow applicants seek orders under s 115A in relation to the following URLs, IP Addresses and Domain Names (which are referred to in their proposed orders in the singular as “the Target Online Location”):

URLs

- https://www.solarmovie.ph;
- https://www.solarmovie.is;
- http://www.solarmovie.com; and
- http://www.solarmovie.eu;

(“the SolarMovie URLs”)

IP Addresses

- 185.47.10.11;
- 205.204.80.87;
- 188.92.78.142; and
- 68.71.61.168;

(“the SolarMovie IP Addresses”)

Domain Names

- www.solarmovie.ph;
- www.solarmovie.is;
- www.solarmovie.com; and
- www.solarmovie.eu.

(“the SolarMovie Domain Names”).

- 60 The evidence relied upon by the Roadshow applicants included an affidavit of Mr Aaron Herps who is the Senior Manager, Global Content Protection for the Motion Picture Association American Inc (“MPAA”), an association that represents the interests of the motion picture industry by (inter alia) seeking to promote and protect its members’ (which includes the third to eighth applicants) intellectual property. He has technical qualifications in computing and telecommunications engineering and experience in relation to website blocking.
- 61 In February 2016 Mr Herps connected a computer to the Internet using a number of carriage services provided by Telstra, Optus, M2 and TPG and entered into the Internet browser the SolarMovie URLs <https://www.solarmovie.is>, <http://www.solarmovie.com> and <http://www.solarmovie.eu>. In each case Mr Herps was automatically directed to the URL, <http://www.solarmovie.ph>.
- 62 Mr Herps conducted a DNS query to determine the IP Addresses of each of the SolarMovie URLs. By this means he established the IP Addresses for each of the SolarMovie URLs which I have referred to above as the SolarMovie IP Addresses. Mr Herps then conducted a search in respect of each of the SolarMovie IP Addresses using MaxMind to ascertain the country code, geographical location, postal code, co-ordinates and ISP associated with each of those IP Addresses. By this means Mr Herps established that each of the SolarMovie IP Addresses is located outside Australia. In particular, he established that IP Addresses 68.71.61.168 and 205.204.80.87 were located in Canada and IP Addresses 185.47.10.11 and 188.92.78.142 were located in Latvia. In oral evidence given at the hearing Mr Herps said that he believed there were four different servers currently hosting the SolarMovie site in two different countries (presumably Canada and Latvia).
- 63 Mr Herps also performed a search of the SolarMovie Domain Names using the Whois service. This search indicated the Domain Name www.solarmovie.com, a generic “top level” domain, is ultimately administered by a US company. The other SolarMovie Domain Names are registered in Iceland (www.solarmovie.is), the European Union (www.solarmovie.eu) and the Philippines (www.solarmovie.ph).
- 64 Mr Herps also carried out an exercise using Google Chrome to determine whether there were any other online locations located at any of the SolarMovie IP Addresses apart from the SolarMovie website. He did this by typing into the address bar of Google Chrome each of the SolarMovie IP Addresses which prompted the Internet browser to generate a “security

error” identifying a mismatch between the IP Address entered into the web browser and what the Internet server was itself identifying as “solarmovie.is”. According to Mr Herps’ evidence, if other websites had been located on that sever or at that IP Address, he would have received a message which indicated that there was more than one website available on that server or for that IP Address.

65 Mr Herps’ evidence establishes that the SolarMovie website provided public access to a large library of motion pictures and television programs. In particular, his evidence includes details of an analysis of the SolarMovie website undertaken by MPAA staff which indicates that there were, as at 1 February 2016, 15,644 motion pictures and 1,768 television series (138,503 episodes) located at the SolarMovie website. Mr Herps was able to access some of these after creating a user account which required him to provide a valid email address, a login ID and a password, and activating his account by means of a link sent to his email address. His evidence makes clear that becoming a registered user is a simple process which requires nothing more than a computer with an Internet connection, a web browser and a valid email address.

66 Mr Herps was also able to use search facilities on the SolarMovie website to search for particular motion pictures and television series. He was able to search for individual titles using a free text search tool or to browse through various categories of movie titles including “New Movies”, “HD Movies”, “Most Popular”, “Latest” and “Coming Soon” and various categories of television programs including “New Episodes”, “Most Popular”, “Latest” and “Coming Soon”. A particular motion picture or television program could then be selected for viewing by clicking on a hyperlink leading to a webpage on which a “Play Now” button appeared. By clicking on this button the viewer was directed to a new webpage (“the streaming page”). Clicking another “play” button on the streaming page activated an embedded player which then streamed the motion picture or television program to the user’s computer where it could be viewed on the computer’s screen. Although streaming causes the motion picture or television program to be displayed on the user’s computer screen, it does not result in the download of a permanent copy.

67 Using the search facility on the SolarMovie website, Mr Herps was able to locate and stream for viewing on his computer screen each of the Roadshow films. Though he did not view each film in its entirety, it is apparent from his evidence that each of them was made available online at the SolarMovie website from which they could be streamed.

68 I am satisfied that the motion pictures and television programs catalogued on the SolarMovie website were available for streaming to computers in Australia with an Internet connection and a web-browser operated by a registered user.

69 I am also satisfied that the primary purpose of the SolarMovie website was to infringe or to facilitate the infringement of copyright in cinematograph films.

The Supplementary Evidence

70 The supplementary evidence relating to the SolarMovie website consisted of further affidavits by the Roadshow applicants' solicitor, Mr Stewart, which indicated that the SolarMovie website was not accessible via any of the SolarMovie URLs, the SolarMovie Domain Names or the SolarMovie IP Addresses as at 22 July 2016 and until at least 14 November 2016 when the last of Mr Stewart's affidavits was sworn.

71 There is nothing before me to explain why the SolarMovie website was taken off-line. Nor is there any evidence to suggest that the present state of affairs as described in the supplementary evidence is permanent or that the operators of the SolarMovie website will not re-activate it at some time in the near future.

Should an injunction be granted?

72 I am satisfied that the SolarMovie website is situated on servers located outside Australia to which each of the respondents provide access.

73 Evidence from Mr Herps establishes that each of the Roadshow films was made available online at the SolarMovie website without the licence of the copyright owner. I am therefore satisfied that by making available online each of the Roadshow films to the public without the licence of the owner of the copyright in such films, the SolarMovie website both infringed and facilitated the infringement of the Roadshow copyright owners' copyright in the Roadshow films.

74 I am also satisfied that the primary purpose of the SolarMovie website is and was, at the time the Roadshow proceeding was commenced, to infringe or facilitate the infringement of copyright. In particular, I am satisfied that the SolarMovie website was designed and operated to facilitate easy and free access to cinematograph films made available online, something which, I would infer, has almost certainly occurred without the permission of the owners of the copyright in such films.

75 On the matter of discretion, I have had regard to the matters referred to in s 115A(5). It is apparent that the SolarMovie website positively encouraged the infringement of copyright on what I am satisfied is likely to be a widespread scale. These activities involved a flagrant disregard for the Roadshow copyright owners' rights, the rights of other copyright owners whose films were made available online at the SolarMovie website, and copyright generally. Blocking orders have already been made in relation to many of the SolarMovie sites in other jurisdictions.

76 I have also had regard to the supplementary evidence. The fact that the SolarMovie website is, or at least appears to have been, off-line since July this year, is a matter relevant to the exercise of the discretion to grant relief under s 115A. However, in the circumstances, I am satisfied that there is a substantial risk that this inactivity is merely temporary and that it does not warrant refusing the Roadshow applicants' relief under s 115A to guard against the possibility that the website will be re-activated at some time in the near future.

77 In all the circumstances I am satisfied that an injunction should be granted in the Roadshow proceeding. I will say more about the terms of the injunction and related orders later in these reasons.

THE FOXTEL PROCEEDING

The Foxtel programs

78 Foxtel claims to be the owner of copyright in the following television programs ("the Foxtel programs"):

- Wentworth (Season 3);
- Open Slather;
- A Place to Call Home (Season 3); and
- Real Housewives of Melbourne (Season 2).

79 None of the respondents put either subsistence or ownership of copyright in issue in the Foxtel proceeding nor did any suggest that it was not open to the applicant to rely upon s 126 in a proceeding under s 115A of the Act. In the absence of any evidence to suggest that Foxtel is not the owner of copyright in the Foxtel programs then subsistence and ownership should be taken to be established.

80 Foxtel seeks orders under s 115A in relation to 61 URLs, IP Addresses and Domain Names which are identified in Appendix A to these reasons. The relevant Domain Names, IP Addresses and URLs in respect of which such relief is sought are arranged into the following four groups:

- The Pirate Bay (Group A);
- Torrentz (Group B);
- TorrentHound (Group C); and
- IsoHunt (Group D).

The Pirate Bay (Group A)

81 When Mr Carson commenced his investigation of The Pirate Bay (“TPB”) using a number of popular web browsers to search for “piratebay”, his searches returned a reference to the URL “https://thepiratebay.la” which, according to Mr Carson, was one of several TPB sites that arose after the suspension of the TPB’s ccLTD for Sweden (“se”). However, by the time he finalised his expert report the primary site for TPB could be found at the URL “https://thepiratebay.se”. This was the site to which Mr Carson was directed when conducting his subsequent Internet searches using popular web browsers and when accessing the Internet via the Internet services provided by Optus and Telstra.

82 Mr Carson identified in his expert report a number of secondary sites for TPB that appear to act as TPB proxy sites that pass requests through to the primary site for TPB. He was able to access these after referring to consolidated lists of TPB secondary sites made available at various TPB sites.

83 Mr Carson was able to identify these proxy sites by using popular web browsers to search for “piratebay” together with additional terms such as “proxy” or “proxies”. He explained in his report that there are many such sites and that these can fluctuate between an active and inactive state.

84 The Domain Names and IP Addresses for each of the TPB secondary sites are identified in Appendix B to Mr Carson’s report together with details of the:

- *Domain Name*: the website domain name, eg thepiratebay.se;
- *IP Address*: the IP Address active for the site, for the inactive TPB Sites described Mr Carson included the last known IP Address he could identify;

- *IP Owner*: the entity allocated the IP Address;
- *IP Location*: the geographic location of the entity allocated the IP Address searches and traceroute searches;
- *Domain Owner*: the entity assigned ownership of the domain name for the website; and
- *Domain Location*: the geographic location of the entity owning the domain name.

85 The Domain Name and IP Address for the primary and each of the secondary sites (37 sites in total including six which Mr Carson describes as inactive) are reproduced and numbered 1 to 37 in Appendix A, Group A, to these reasons. According to Mr Carson's evidence, Domain Names numbered 20, 25-28 (inclusive) and 31 were inactive at the time he prepared his report.

86 Virtually all of the Group A IP Addresses referred to in Mr Carson's Appendix B were, as at 5 February 2016, allocated to CloudFlare. The only exception to this is one of the inactive sites (20) which is shown to have an IP Address allocated to Search Guide Inc. In his report, Mr Carson expresses the opinion that it is highly likely that each of the primary TPB websites and each of the secondary TPB websites are located outside Australia. His opinion on this issue is largely based upon the involvement of CloudFlare which is based in the United States.

87 Mr Carson is also of the opinion that the primary purpose of each of the TPB sites is to provide users with free access to copyright material including motion pictures, television programs and computer software. This includes recently released motion pictures and television programs many of which he says are not yet available in Australia.

88 Mr Carson describes in his report how he accessed an electronic copy of an episode of the television program known as "Wentworth" using a computer on which uTorrent (a BitTorrent client) was installed. He performed a search using a web browser for "the pirate bay" which produced a search result headed "Download music, movies, games, software! The Pirate Bay" together with a link to the URL <https://thepiratebay.se/>". By clicking on this link Mr Carson was able to connect to the TPB website. He then searched for "wentworth" using a search facility at the TPB website. This search generated various search results consisting of various magnet links associated with various torrent files including torrent files used to

download episodes of Wentworth, Season 3. The download information on the user's screen which is reproduced in Mr Carson's report includes details of the time and date on which torrent files were uploaded. This suggests that the TPB site allows users to upload torrent files which may then be accessed by other users.

- 89 The evidence includes an affidavit made by Ms Blunt, a lawyer engaged by the solicitors for Foxtel, covering a number of matters including searches she undertook of various websites and attaching various screenshots which she took. At the webpage <https://thepiratebay.se/about> the following statement appeared:

The Pirate Bay is the worlds largest bittorrent indexer. Bittorrent is a filesharing protocol that in a reliable way enables big and fast file transfers.

No torrent files are saved on the server. That means no copyrighted and/or illegal material are stored by us. It is therefore not possible to hold the people behind The Pirate Bay responsible for the material that is being spread using the site.

The Pirate Bay was started by the swedish anti copyright organization Piratbyran in the late 2003, but in October 2004 it separated became run by dedicated individuals. In 2006 the site changed its ownership yet again. Today the site is run by an organisation rather than individuals, though as a non-profit. The organisation is registered in the Seychelles and can be contacted using the contact form.

Using the site is free of charge for individuals however there are some restrictions. Please see the policy page.

(Errors original)

- 90 Ms Blunt's screenshots also show catalogued indexes of many popular and well-known sound recordings, motion pictures, television programs and computer software (including well-known business applications and popular games). The television programs include episodes of Wentworth (Seasons 1, 2 and 3), Open Slather (Season 1), A Place to Call Home (Seasons 1, 2 and 3) and Real Housewives of Melbourne (Seasons 1 and 2). I am satisfied that each of these television programs, copyright in which is in some cases owned by Foxtel, can be downloaded by a BitTorrent client via a magnet link and/or associated torrent file located on the primary website found at the URL <https://thepiratebay.se> and, I infer, via various secondary sites that are identified in Mr Carson's report. There is also evidence from Mr Crowley, the Director of Content and Movies at Foxtel, which satisfies me that the Foxtel programs were made available online without the licence of the copyright owner.
- 91 Ms Blunt's evidence also shows that blocking orders have been made in relation to various TPB sites by orders of courts in various jurisdictions, including in the United Kingdom.

92 Further evidence was provided by Mr Southey, the Technology Development Manager – Security and Compliance at Foxtel. It is not necessary to refer to all of his evidence which includes a large number of screenshots recording steps taken by him when investigating various TPB sites in January 2016 using internet services provided by Telstra, Optus and TPG. His evidence is consistent with other evidence to which I have referred. It also demonstrates that the TPB sites investigated by him do not include any effective facility which may be used to communicate with the operator or to deliver a “take down” notice.

Should an injunction be granted?

93 As I have previously mentioned, the TPB sites in relation to which Foxtel seeks an order under s 115A include what Mr Carson described as “inactive sites” being those TPB Domain Names, IP Addresses and URLs that he established either did not resolve to a website at all or resolved to a website that appeared to be unrelated to the active websites.

94 Each of the inactive sites has a Domain Name that includes the name “thepiratebay” and, with one exception, is also shown to be associated with an IP Address allocated to CloudFlare. The one exception is the Domain Name “thepiratebay.am” which uses the country code TLD for Armenia, and an IP Address allocated to a corporation called Search Guide Inc. Although the Domain Names for the inactive sites and the CloudFlare involvement give rise to a strong suspicion that they have been used to infringe or facilitate the infringement of copyright, I do not think this provides a sufficient basis for holding that the s 115A requirements have been satisfied. There is simply no evidence before me to show that these particular online locations have ever infringed or facilitated the infringement of copyright.

95 It follows that I will not grant relief in relation to the inactive TPB sites. Of course, it is open to Foxtel to apply for a further injunction or an extension of any injunction that is granted in relation to the other TPB sites (including the inactive sites), at a later date in the event there is a relevant change in circumstances.

96 With respect to the primary site and each of the active secondary sites, I am satisfied that it is appropriate to grant an injunction under s 115A. In each case I am satisfied of the matters referred to in s 115A(1). Each site, which I am satisfied is located outside Australia, facilitates the infringement of copyright, including Foxtel’s copyright in the Foxtel programs, which can be downloaded using magnet links found there. The fact that copyright material may not be stored at any of the TPB sites does not lead to any different conclusion. The TPB

sites provide BitTorrent clients with what can be likened to a trigger which, when pulled, causes the swarm to download copyright material (whether it be a film, a sound recording or a computer program) to a computer running a BitTorrent client.

97 I am also satisfied that the primary purpose of each of the active TPB sites is to facilitate the infringement of copyright. This is clear from the statements appearing on the primary site (to which I have referred) and the nature and extent of the copyright material that is available for download using the magnet links and/or torrent files found there.

98 In relation to the matter of the discretion, I am satisfied that the facilitation of the infringement of copyright is flagrant, and that the operator of the TPB sites has shown a blatant and wilful disregard for the rights of copyright owners. As I have also mentioned, blocking orders have already been made in relation to many of the TPB sites in other jurisdictions. I am satisfied that it is appropriate to grant an injunction under s 115A in respect of each of the active TPB sites.

Torrentz (Group B)

99 At the time Mr Carson completed his expert report the website known as “Torrentz” had its primary site located at <http://torrentz.eu>. This is the site to which Mr Carson was directed when he conducted searches for “torrentz” using well-known web browsers.

100 The secondary Torrentz sites, which are numbered 2-11 (inclusive) in Appendix A, Group B, all have Domain Names that refer to “torrentz”, “torrentzmirror” or the abbreviation “tz”.

101 Appendix B to Mr Carson’s report shows that the primary site, <http://torrentz.eu>, has an IP Address allocated to CloudFlare and that the owner of the Domain Name torrentz.eu is “Majewski Karol”. The owner of the IP Address associated with each of the secondary sites is an entity known as Inventoris Sp. z o. o which appears to be based in Poland. “Majewski Karol” is also shown as the owner of the Domain Name for each of the secondary sites except for two.

102 Mr Carson was able to use the search engine found at the primary site to download a copy of Wentworth, Episode 3, Series 3. He inspected each of the secondary sites and was able to establish that they also provided a search engine which enabled him to locate the relevant link for the same episode of Wentworth indicating that it was also accessible via the secondary site.

- 103 Ms Blunt's evidence includes copies of screenshots taken by her of various webpages at the Torrentz sites. The screenshots of the primary site includes statements indicating that it is a free, fast and powerful search engine that combines results from dozens of other search engines indexing 32,487,111 active torrent files. There are also statements indicating that Torrentz does not store copyright material, that it does not host or make available torrent files, and that it merely acts as a search engine that can be used by members to link to other search engines that might host torrent files.
- 104 When Ms Blunt used Torrentz to search for "Wentworth" a listing of torrent files that could be used to trigger the download to a BitTorrent client of various episodes of Wentworth appeared including episodes from Seasons 1, 2 and 3. Her searches for "A Place to Call Home" and "Real Housewives of Melbourne" produced similar listings of episodes for each of those television series. There is also evidence from Mr Crowley who conducted searches for those television programs and "Open Slather". All of these searches returned links to torrent files which could be used by a BitTorrent client to download copies of many different episodes.
- 105 The webpages reproduced in Ms Blunt's evidence also include a list of sites in the Torrentz index. The list includes references to about 26 other sites including "thepiratebay.se" (64,886 torrents) "thepiratebay.org" (3,363,945 torrents), "torrenthound.com" (8,321,919 torrents) and "isohunt.to" (6,159,571 torrents). It can be inferred that the motion pictures and television programs that could be downloaded from swarms using magnet links and/or torrent files available at these other sites were accessible using links appearing on the Torrentz sites.
- 106 There is also evidence from Ms Blunt that indicates that a Torrentz website was the subject of a blocking order made in the United Kingdom in respect of the website located at the Domain Name www.torrentz.cd, although that particular Domain Name is not one of those in respect of which relief is sought in this case.
- 107 The supplementary evidence indicated that, as at 10 November 2016, the Torrentz sites were still online and accessible. However, the home page of each such site included a statement "Torrentz *was* a free, fast and powerful metasearch engine [etc]" (my emphasis) and a farewell message. In addition, the search function, though still appearing on the page, was not returning any results in response to search requests.

Should an injunction be granted?

108 In the case of the Torrentz sites I am satisfied that the requirements of s 115A(1) are satisfied. In particular, I am satisfied that each of them is located outside Australia, and that they have facilitated the infringement of copyright, including the applicant's copyright, by providing links to torrent files located on other sites, including TPB, which infringe or facilitate the infringement of copyright. This has enabled BitTorrent clients to download copyright material, including many well-known films and television programs, made available online for free and unrestricted distribution, without the permission of copyright owners.

109 I am satisfied that the primary purpose of the Torrentz sites is to facilitate the infringement of copyright.

110 I have already considered the meaning of the words used in s 115A(1)(a) and (b) from the temporal perspective when discussing the supplementary evidence relating to the SolarMovie sites. The fact that the supplementary evidence suggests that the search engine on the Torrentz sites is not currently enabled does not preclude the making of an order under s 115A in respect of the Torrentz sites.

111 On the question of discretion, I am satisfied that the facilitation of copyright infringement by the Torrentz sites was flagrant, and that the operator has shown a blatant disregard for the rights of copyright owners. I am not satisfied that the search facilities on the Torrentz sites have been permanently disabled or that the current state of affairs as disclosed in the supplementary evidence is anything other than temporary. In the circumstances, I am satisfied that it is appropriate to grant an injunction under s 115A in respect of each of the Torrentz sites.

TorrentHound (Group C)

112 At the time Mr Carson prepared his report, the primary site for TorrentHound was www.torrenthound.com which is the site to which he was directed when conducting searches for TorrentHound using popular web browsers. His investigations disclosed the existence of six secondary sites. The Domain Names, IP Addresses and URLs for the primary and each of the secondary TorrentHound sites appear in Appendix A, Group C.

113 At each of the TorrentHound sites, Mr Carson was able to use the search facility provided to locate a magnet file for an episode of Wentworth.

- 114 Mr Carson's report indicates that the owner of the IP Addresses for five of the TorrentHound secondary sites is CloudFlare. Other ownership information relating to the TorrentHound sites, including the primary site, reveal connections with Sweden, Estonia and the United Kingdom. All such information suggests that each of the TorrentHound sites is located outside Australia.
- 115 Screenshots of searches undertaken by Ms Blunt at the TorrentHound primary site indicate that it included many magnet links to torrent files for popular motion pictures and television programs including episodes of Wentworth, Open Slather, Real Housewives of Melbourne and A Place to Call Home. At least some of these programs appear to be available by direct download from the site without any need to use a BitTorrent client.
- 116 Mr Southey's evidence also shows that many different copies of the Foxtel programs were available for download free of charge either directly or via magnet links on the TorrentHound primary site as well as many popular motion pictures such as The Revenant, The Martian, The Intern and The Good Dinosaur. I am satisfied that all of these were being made available for download (whether directly or using a BitTorrent client) without the permission of any of the copyright owners.
- 117 The supplementary evidence indicated that, as at 10 November 2016, it was still possible to use the search facility to locate and download Foxtel programs from the site torrenthound.to (ccTLD Tonga).

Should an injunction be granted?

- 118 In the case of the TorrentHound sites I am satisfied that the requirements of s 115A(1) are satisfied. I am satisfied that each of the sites is an online location situated outside Australia that has as its primary purpose the facilitation of copyright infringement. Blocking orders have already been made in relation to many of the TorrentHound sites in other jurisdictions. I am also satisfied that the TorrentHound sites have facilitated the infringement of copyright, including Foxtel's copyright, on a widespread scale, in flagrant disregard of the rights of copyright owners generally. I am satisfied that an injunction should be granted under s 115A in respect of the TorrentHound sites.

IsoHunt (Group D)

- 119 Mr Carson identified the primary site for IsoHunt as that found at <http://isohunt.to> which is the URL to which he was directed when searching for IsoHunt using popular web browsers.

CloudFlare appears to be the owner of the IP Addresses for the primary site. The primary site and each of the secondary sites appear to be located outside Australia. At each of the IsoHunt sites Mr Carson was able to use the search facility provided to locate the same magnet file as was available at each of the TorrentHound sites.

120 Ms Blunt's evidence includes screenshots of the IsoHunt website accessible at isohunt.to which show large numbers of torrent files on the site facilitating free and unrestricted access to popular television programs and motion pictures including The Walking Dead, The Big Bang Theory, Homeland, Three Kings, Lost in Translation, Changeling, LA Confidential, Die Hard, Blue Lagoon and many more. Her screenshots also show torrent files for Wentworth, Open Slather, A Place to Call Home and Real Housewives of Melbourne.

121 Ms Blunt's evidence shows that an order was made by the High Court of Justice in England on 19 November 2014 requiring various ISPs to take steps to block customers' access to the website accessible at isohunt.to known as IsoHunt.

122 Mr Southey's evidence shows that the IsoHunt sites provide a facility that enables users to receive a notification when particular content which they are interested in is added and available for viewing. The primary site includes the following statements:

New category tags and TV Series. July update.

Yo! Summer is at it's peak and we hope you're having a great time. We are not, because we're working to make Isohunt.to better. Some quick update this month.

Some of you might know that now you can subscribe Movies and TV Shows to get notifications. If not, you can Learn more about Notifications here. We made this chart of a new movies that you may want to subscribe. Some of them are in theaters now, some of them will soon be. Subscribe and be the first one to watch them!

[...]

We got tags in 4 categories Software Games Books and Music. You asked for 'em and you got 'em. Hope it'll help you to find content better and faster

We added about 40,000 of TV Series! So if you had any problems with finding your favorite show, try again and maybe you're in luck this time.

Now you don't need to search for your favorite content (movies and shows for the moment)! When entering the website you simply will get notifications! Or if you are a busy man, just wait for that email to come and you don't even need to enter the website before the content is uploaded

For Movies you need to choose Any or Good quality you want to get notifications of

With Any you will get content faster but with lower quality + good quality. With Good it takes more time but quality is a lot better

For TV Shows you need to choose.

What specific Season and Episode you want to start follow it Or get notifications of Any uploaded episode.

(Errors original, emphasis omitted).

Should an injunction be granted?

123 In the case of the IsoHunt sites I am satisfied that the requirements of s 115A(1) are satisfied. I am satisfied that each of the sites is an online location situated outside Australia that has as its primary purpose the facilitation of copyright infringement. I am also satisfied that the IsoHunt sites have facilitated the infringement of copyright, including Foxtel's copyright, on a widespread scale, in flagrant disregard of the rights of copyright owners generally. I am satisfied that an injunction should be granted under s 115A in respect of the IsoHunt sites.

TERMS OF RELIEF

124 As previously mentioned, the parties were agreed on most matters relating to the form of the injunctive relief that should be granted in the event that the Court was satisfied that these were proper cases for the grant of relief under s 115A of the Act. It is convenient to deal with each of the remaining issues that were not agreed in the sequence in which they are raised in Foxtel's proposed orders. The Roadshow applicants' proposed orders are not materially different except in so far as they define "Target Online Location", "Target URLs", "Target IP Addresses" and "Target Domain Names".

Orders 1 to 7

125 The applicants' proposed orders 1 to 7 are in these terms (after correction of some errors):

1. Each respondent must, within 15 business days of these orders, take reasonable steps to disable access to the Target Online Location.
2. Order 1 is taken to have been complied with by a respondent if that respondent implements any one or more of the following steps:
 - (a) Order 1 is taken to have been complied with by a respondent if that respondent implements any one or more of the following steps:
 - (b) IP Address blocking or re-routing in respect of the Target IP Addresses;
 - (c) URL blocking in respect of the Target URLs and the Target Domain Names; or
 - (d) any alternative technical means for disabling access to a Target Online Location as agreed in writing between the applicants and a respondent.
3. If a respondent in complying with order 1 does not implement one of the steps

referred to in order 2, that respondent must, within 15 business days of these orders, notify the applicants of the step or steps it has implemented.

4. Each respondent must redirect any communication by a user of its service seeking access to a Target Online Location which has been disabled pursuant to order 1 to a webpage established, maintained and hosted by either:
 - (a) the applicants, or their nominee, pursuant to order 5; or
 - (b) that respondent or its nominee.

The applicants' obligations pursuant to orders 5 and 6 only arise if a respondent notifies the applicants that the respondent will redirect a communication pursuant to order 4(a) and for so long as at least one respondent redirects communications to that webpage.

5. The applicants, or their nominee, must establish, maintain and host a webpage which informs users of a respondent's service who have been redirected to the webpage pursuant to order 4 that access to the website has been disabled because this Court has determined that it infringes or facilitates the infringement of copyright.
6. Within 5 business days of these orders, the applicants will notify each of the respondents in writing of the URL of the webpage established, maintained and hosted under order 5 and, if the webpage ceases to operate for any reason, will notify each of the respondents in writing of a different URL that complies with order 5.
7. If, in complying with order 4, a respondent redirects any communication by a user of its service to a webpage established, maintained and hosted by it, that respondent or its nominee must ensure that the webpage informs the user of that respondent's service that access to that the website has been disabled because this Court has determined that it infringes or facilitates the infringement of copyright.

126 There is a minor issue between the applicants and some of the respondents as to whether proposed order 4 should require each respondent to direct communications to a webpage established, maintained and hosted by either the applicants or their nominee or the respondents or their nominee. Telstra submitted that this should be optional rather than mandatory.

127 The Revised Explanatory Memorandum expressly anticipates that the Court might see fit to require the establishment of a landing page at [43]:

... to ensure that subscribers are informed of the reason that they are unable to access a disabled online location, avoiding the need to contact their CSP for information.

128 It seems to me desirable that either the applicants or the respondents establish and maintain a landing page in accordance with the applicants' proposed orders to which each ISP's customers may be redirected when they attempt to communicate with the blocked sites and

which will inform them of the reason why they are unable to establish a connection. If an ISP does not wish to incur the cost of establishing its own landing page then its customers can be redirected to the webpage established by the applicants pursuant to proposed order 5.

Order 8

129 The applicants' proposed order 8 is in these terms:

8. In the event that the applicants have a good faith belief that:
 - (a) any Target URL, Target IP Address or Target Domain Name which is subject to these orders has permanently ceased to enable or facilitate access to a Target Online Location; or
 - (b) any Target URL, Target IP Address or Target Domain Name has permanently ceased to have the primary purpose of infringing or facilitating the infringement of copyright,a representative of the applicants must, within 15 business days of the applicants forming such a good faith belief, notify each respondent of that fact in writing, in which case the respondents shall no longer be required to take steps pursuant to order 1 to disable access to the relevant Target URL, Target IP Address or Target Domain Name that is the subject of the notice.

130 There is agreement in relation to the applicants' proposed order 8. In my view it is an appropriate order to make.

Order 9

131 The applicants' proposed order 9 is in these terms:

9. A respondent will not be in breach of order 1 if it temporarily declines or temporarily ceases to take the steps ordered in order 1 (either in whole or in part) upon forming the view, on reasonable grounds, that suspension is necessary to:
 - (a) maintain the integrity of its network or systems, or functioning of its blocking system;
 - (b) upgrade, troubleshoot or maintain its blocking system;
 - (c) avert or respond to an imminent security threat to its network or system; or
 - (d) ensure the reliable operation of its ability to block access to online locations associated with criminal content if it reasonably considers that such operation is likely to be impaired, or otherwise to comply with its statutory obligations including under section 313(3) of the *Telecommunications Act 1997* (Cth)

provided that:

- (e) unless precluded by law, it notifies the applicants or their legal

representative(s) of such suspension, including the reasons and the expected duration of such suspension by 5.00 pm on the next business day; and

- (f) such suspension lasts no longer than is reasonably necessary and, in any case, no longer than 3 business days.

132 There is a minor disagreement between the applicants and Telstra as to the terms of subpara (f). The parties agree that any suspension that is to occur pursuant to this order should not last longer than is reasonably necessary but the applicants submit that the order should expressly limit any suspension to three days. Telstra opposes this additional limitation on the basis that the requirement that the suspension last “no longer than is reasonably necessary” is reasonable and sufficient.

133 I prefer the applicants’ formulation which provides a desirable measure of certainty in relation to the operation of order 9. In the event that the respondents require more than three days then it is open to them to apply to the Court for an extension of time. To that end, I propose to vary the applicants’ proposed form of order by adding to the end of subpara (f) the words “or such longer period as the applicants may agree in writing or the Court may allow.”

Orders 10 and 11

134 The applicants’ proposed orders 10 and 11 are in these terms:

10. The owner or operator of a Target Online Locations and the owner or operator of any website who claims to be affected by these orders may apply on 3 days’ written notice, including notice to all parties, to vary or discharge these orders, with any such application to:
 - (a) set out the orders sought by the owner or operator of the Target Online Locations or affected website; and
 - (b) be supported by evidence as to:
 - (i) the status of the owner or operator of the Target Online Locations or affected website; and
 - (ii) the basis upon which the variation or discharge is sought.
11. The parties have liberty to apply on 3 days’ written notice, including, without limitation, for the purpose of any application:
 - (a) for further orders to give effect to the terms of these orders;
 - (b) for further orders in the event of any material change of circumstances including, without limitation, in respect of the consequences for the parties and the effectiveness of the technical methods under order 1; and/or
 - (c) for orders relating to other means of accessing a Target Online

Locations not already covered by these orders.

135 The applicants' proposed orders 10 and 11 are agreed and are in my view appropriate.

Orders 12-16

136 Orders 13 to 16 are essentially agreed. Order 12, in the form proposed by all respondents, is not agreed to by the applicants which seek a different order (the applicants' proposed order 12) permitting them to extend the scope of proposed order 1 to Domain Names, IP Addresses and URLs that are not presently specifically referred to by giving written notice to the respondents without any further order of the Court. Proposed orders 12 to 16, in the terms that the respondents favour, are as follows:

12. If the website the subject of a Target Online Locations is at any time during the operation of these orders provided from a different Domain Name, IP Address or URL:
 - (a) The applicants may file and serve;
 - (i) an affidavit which:
 - (A) identifies the different Domain Name, IP Address or URL;
 - (B) states that, in the good faith belief of the deponent, the website operated from the different Domain Name, IP Address or URL is a new location outside Australia for the Target Online Locations the subject of these orders and brief reasons therefor; and
 - (ii) proposed short minutes of order to the effect that:
 - (A) The definition of Target Online Locations in these orders is amended to include the different Domain Name, IP Address or URL; and
 - (B) The time period in order 1 of these orders starts to run in relation to the different Domain Name, IP Address or URL upon service in accordance with order 16(d) of the orders as made.
13. These orders are to operate for a period of 3 years from the date of these orders.
14. Six months prior to the expiry of these orders:
 - (a) the applicants may file and serve:
 - (i) an affidavit which states that, in the good faith belief of the deponent, a Target Online Locations continues to have the primary purpose of infringing or facilitating the infringement of copyright; and
 - (ii) short minutes of order extending the operation of these orders

for a further 3 year period; and

(b) the process contained in order 16 shall apply.

15. The affidavits referred to in orders 12 and 14 is to be given by a deponent duly authorised to give evidence on behalf of the applicants and may be given by their solicitor.

16. If an affidavit and short minutes of order are filed and served in accordance with orders 12 or 14:

(a) within 7 business days, the respondents must notify the applicants and the Court if they object to the orders being made in accordance with the short minutes of orders served by the applicants;

(b) if any respondent gives notice of any objection, or the Court otherwise thinks fit, the proceeding will be relisted for further directions;

(c) if no respondent gives notice of any objection and the Court does not otherwise require the proceeding to be relisted, then the Court may make orders in terms of the short minutes of orders served by the applicants without any further hearing; and

(d) the applicants must serve on the respondents any such orders made.

137 In my view the respondents' proposed order 12 is preferable. Whether the terms of any injunction should be varied to refer to additional Domain Names, IP Addresses or URLs is a matter for the Court to determine in light of evidence.

138 The applicants submitted that notifications of the kind they propose will not amount to variations to the injunction because they will be provided for by the terms of the orders the applicants propose. However, the effect of a notice given by the applicants under their proposed orders will require the respondents to block additional Domain Names, URLs or IP Addresses which might not point to any of the same online locations in relation to which the injunction was originally granted. If the injunction is to apply to new Domain Names, URLs or IP Addresses, then these are matters which should be dealt with by way of further order in the manner proposed by the respondents.

139 Another submission made by the applicants to the effect that the costs and inconvenience involved in following the procedure outlined in the respondents' proposed order 12 would be excessive or disproportionate was in my view exaggerated and, in any event, not to the point in circumstances where the legislature has specifically identified the matters upon which the Court must be satisfied before it may grant an injunction under s 115A in respect of an online location. In the case of a variation to an existing injunction, the Court may be willing to act

on very little in the way of further evidence. Nevertheless, whether or not there should be such a variation remains a matter for the Court.

Order 17

140 The applicants propose that the respondents bear their own costs of complying with order 1. This approach is opposed by all respondents.

141 Telstra seeks to recover costs it has incurred in configuring its various systems to facilitate compliance with any order that might be made under s 115A of the Act. For the purposes of the following discussion I shall refer to these costs as “set-up costs”. It appears that Telstra incurred set-up costs some time in late 2015 and early 2016 not long after s 115A of the Act came into operation.

142 None of the other respondents sought set-up costs although TPG said that if the applicants were required to pay any other respondents’ set-up costs, then TPG sought them too. Telstra’s set-up costs total \$10,261 and TPG’s total \$21,195.

143 I do not propose to require the applicants to pay Telstra’s set-up costs. These costs, which have already been incurred, will permit Telstra to comply with orders made not only in these proceedings, but in any future proceeding brought by the same or different applicants.

144 It seems to me that given the legislative environment in which the respondents have operated since the introduction of s 115A, it is not merely desirable but, practically speaking, essential that a CSP possess the technical capacity to comply with an injunction in the form agreed in these proceedings. Telstra’s set-up costs are, in my opinion, a general “cost of carrying on business” to borrow an expression used in the English authorities that have considered this question: see *Twentieth Century Fox Film & Ors v British Telecommunications plc* [2011] EWHC 2714 (Ch) at [32] per Arnold J. Moreover, they represent costs which I am satisfied Telstra would at some stage have had to incur irrespective of the existence of these proceedings.

145 All respondents sought orders for the payment by the applicants of various other costs of complying with the proposed orders. These costs, which I shall refer to as compliance costs, essentially reflect what are said to be the costs (excluding any profit component) of making the necessary entries in their DNS Blocking Systems to ensure that DNS blocking of the designated Domain Names is achieved.

- 146 The respondents drew an analogy between compliance costs that will be incurred by them in complying with injunctions granted under s 115A and costs incurred by a person against whom an order is made for preliminary discovery (against whom a substantive proceeding is not commenced) or an order requiring the production of documents (eg. a subpoena for production). The respondents say that they are to be treated as innocent parties against whom relief is sought not by reason of any wrongdoing on their part, but in order to assist the applicants in their efforts to prevent the operators of the relevant online locations from infringing or facilitating the infringement of their copyright.
- 147 The applicants submitted that this analogy was inapt because the respondents benefited commercially from online copyright infringement. This was denied by the respondents who also submitted that the applicants' submission is not supported by any evidence in these proceedings. On the latter point I think the respondents are correct. I therefore do not accept the applicants' submission that the respondents have obtained a commercial benefit by providing access to the relevant online locations or to any other websites that actively encourage copyright infringement. I generally accept the respondents' submissions in relation to compliance costs. I think the applicants should be required to pay the respondents' compliance costs or some significant proportion thereof.
- 148 In circumstances where each of the respondents propose to use DNS Blocking, it seems to me that it is appropriate to settle upon a uniform amount for compliance costs calculated by reference to the number of Domain Names that the respondents will be required to block. For some respondents, this may produce a figure that is slightly below their estimated compliance costs, while others might receive something slightly in excess of their estimated costs. However, the advantage of using a formula of this kind is that all parties know precisely how much they are required to pay and how much they are entitled to receive both now and in the future in the event that the number of Domain Names that the respondents are required to block increases.
- 149 I think an amount of \$50 (exclusive of GST) per Domain Name is appropriate. This equates to \$200 (\$50 x 4) for each grouping of respondents in the Roadshow proceeding and \$2,750 (\$50 x 55) for each grouping of respondents in the Foxtel proceeding. The figure of \$50 per Domain Name broadly reflects the amount sought by TPG, but is less than the amount sought by Telstra and M2. To the extent that the respondents may incur compliance costs in excess of what I have allowed then I think they should be left to bear them. In the Foxtel proceeding

Optus and Foxtel agreed that \$1,500 was an appropriate amount. My orders will reflect that agreement.

“No Fault” Notation

150 TGP submitted that the minute of the Court’s orders should include a notation to the following effect:

No allegation was made by the Applicants that any Respondent had itself infringed copyright or otherwise engaged in any wrongdoing and the Respondents submitted to the following orders without any admission of liability of their part.

151 The proposed notation is factually correct, but I am not persuaded that it should be included in the minutes of the orders.

Costs

152 The applicants did not seek any costs. Each of the respondents sought orders that the applicants pay its costs of the proceeding.

153 As I previously mentioned, the parties were able to agree on a number of matters pertaining to the form of the injunctions and the related orders. These matters of agreement were no doubt the product of extensive negotiation between the applicants and the respondents all of whom have a significant commercial interest in working out and, if possible, agreeing upon, suitable forms of orders that might be made in these and in other proceedings brought by copyright owners pursuant to s 115A of the Act. In my view the parties should bear their own costs in relation to all matters that were the subject of agreement.

154 There were two significant issues in contest between the parties upon which the respondents succeeded: the first related to the applicants’ proposed order allowing for the giving of written notices with a view to extending the scope of the injunctions (the applicants’ proposed order 12), and the second related to the matter of compliance costs. In my view the applicants, which were wholly unsuccessful in relation to the first of these matters, and largely unsuccessful in relation to the matter of compliance costs, should be required to pay the respondents’ costs with respect to these issues.

155 The costs orders I propose to make in each proceeding will require the applicants to pay the respondents’ costs of and incidental to the preparation of evidence and written submissions, and the making of oral submissions, in relation to the applicants’ proposed order 12 and the

issue of compliance costs (excluding set-up costs). There will also be an order in each proceeding that there be no other order as to costs.

156 There will be orders accordingly.

I certify that the preceding one hundred and fifty-six (156) numbered paragraphs are a true copy of the Reasons for Judgment herein of the Honourable Justice Nicholas.

Associate:

Dated: 15 December 2016

SCHEDULE OF PARTIES

NSD 239 of 2016

Applicants

Third Applicant:	DISNEY ENTERPRISES, INC
Fourth Applicant:	TWENTIETH CENTURY FOX FILM CORPORATION
Fifth Applicant:	PARAMOUNT PICTURES CORPORATION
Sixth Applicant:	COLUMBIA PICTURES INDUSTRIES, INC
Seventh Applicant:	UNIVERSAL CITY STUDIOS LLC
Eighth Applicant:	WARNER BROS. ENTERTAINMENT INC.

Respondents

Third Respondent:	PACNET SERVICES (A) PTY LTD ACN 056 783 852
Fourth Respondent	OPTUS MOBILE PTY LIMITED ACN 054 365 696
Fifth Respondent	OPTUS NETWORKS PTY LIMITED ACN 008 570 330
Sixth Respondent	UECOMM PTY LIMITED ACN 079 083 195
Seventh Respondent	OPTUS FIXED INFRASTRUCTURE PTY LIMITED (FORMERLY XYZED PTY LIMITED) ACN 092 450 783
Eighth Respondent	UECOMM OPERATIONS PTY LIMITED ACN 093 504 100
Ninth Respondent	VIVIDWIRELESS PTY LIMITED ACN 137 696 461
Tenth Respondent	VIVIDWIRELESS GROUP LIMITED ACN 008 082 737
Eleventh Respondent	VIRGIN MOBILE (AUSTRALIA) PTY LIMITED ACN 092 726 442
Twelfth Respondent	ALPHAWEST PTY LIMITED ACN 009 222 931
Thirteenth Respondent	OPTUS WHOLESALE PTY LIMITED ACN 092 227 551
Fourteenth Respondent	OPTUS CONSUMER/OPTUS INTERNET PTY LIMITED ACN 083 164 532
Fifteenth Respondent	OPTUS BACKBONE INVESTMENTS PTY LIMITED ACN 083 164 532

Sixteenth Respondent	M2 WHOLESALE PTY LTD ABN 99 119 220 843
Seventeenth Respondent	M2 WHOLESALE SERVICES PTY LTD ACN 119 220 843
Eighteenth Respondent	M2 COMMANDER PTY LTD ACN 136 950 082
Nineteenth Respondent	PRIMUS NETWORK (AUSTRALIA) PTY LTD ACN 109 142 216
Twentieth Respondent	PRIMUS TELECOMMUNICATIONS PTY LTD ACN 071 191 396
Twenty First Respondent	PRIMUS TELECOMMUNICATIONS (AUSTRALIA) PTY LTD ACN 061 754 943
Twenty Second Respondent	DODO SERVICES PTY LTD ACN 158 289 331
Twenty Third Respondent	ENGIN PTY LTD ACN 080 250 371
Twenty Fourth Respondent	EFTEL CORPORATE PTY LTD ACN 154 634 054
Twenty Fifth Respondent	EFTEL RETAIL PTY LTD ACN 092 667 126
Twenty Sixth Respondent	EFTEL WHOLESALE PTY LTD ACN 123 409 058
Twenty Seventh Respondent	CLUBTELCO PTY LTD ACN 144 488 620
Twenty Eighth Respondent	WHOLESALE COMMUNICATIONS GROUP PTY LTD ACN 109 626 011
Twenty Ninth Respondent	2TALK PTY LTD ACN 161 656 499
Thirty Second Respondent	TPG INTERNET PTY LTD ACN 068 383 737
Thirty Fourth Respondent	TPG NETWORK PTY LTD ACN 003 064 328
Thirty Fifth Respondent	FTTB WHOLESALE PTY LTD ACN 087 533 328
Thirty Sixth Respondent	CHARIOT PTY LTD ACN 088 377 860
Thirty Seventh Respondent	CHARIOT PTY LTD ACN 088 377 860
Thirty Eighth Respondent	SPT TELECOMMUNICATIONS PTY LIMITED ACN 099 173 770
Thirty Ninth Respondent	SPTCOM PTY LIMITED ACN 111 578 897
Fortieth Respondent	SOUL COMMUNICATIONS PTY LTD ACN 085 089 970
Forty First Respondent	PIPE NETWORKS PTY LIMITED ACN 099 104 122

Forty Second Respondent	INTRAPower TERRESTRIAL PTY LTD ACN 081 193 259
Forty Third Respondent	IINET LIMITED ACN 068 628 937
Forty Fourth Respondent	INTERNODE PTY LTD ABN 82 052 008 581
Forty Fifth Respondent	TRANSACT CAPITAL COMMUNICATIONS PTY LTD ACN 093 966 888
Forty Sixth Respondent	TRANSACT VICTORIA COMMUNICATIONS PTY LTD ACN 063 024 475
Forty Seventh Respondent	WESTNET PTY LTD ACN 086 416 908
Forty Eighth Respondent	ADAM INTERNET PTY LTD ACN 055 495 853
Forty Ninth Respondent	AAPT LIMITED ACN 052 082 416
Fiftieth Respondent	REQUEST BROADBAND PTY LTD ACN 091 530 586

NSD 241 of 2016**Respondents**

Third Respondent:	OPTUS NETWORKS PTY LTD ACN 008 570 330
Fourth Respondent	OPTUS MOBILE PTY LTD ACN 054 365 696
Fifth Respondent	UECOMM PTY LTD ACN 079 083 195
Sixth Respondent	OPTUS FIXED INFRASTRUCTURE PTY LTD ACN 092 450 783
Seventh Respondent	UECOMM OPERATIONS PTY LTD ACN 093 504 100
Eighth Respondent	VIVIDWIRELESS PTY LTD ACN 137 696 461
Ninth Respondent	VIVIDWIRELESS GROUP LTD ACN 008 082 737
Tenth Respondent	VIRGIN MOBILE (AUSTRALIA) PTY LTD ACN 092 726 442
Eleventh Respondent	ALPHAWEST PTY LTD ACN 009 222 931
Twelfth Respondent	OPTUS WHOLESALE PTY LTD ACN 092 227 551
Thirteenth Respondent	OPTUS INTERNET PTY LTD ACN 083 164 532
Fourteenth Respondent	OPTUS BACKBONE INVESTMENTS PTY LTD ACN 136 676 356

Fifteenth Respondent	TELSTRA CORPORATION LTD ACN 051 775 556
Sixteenth Respondent	PACNET SERVICES (A) PTY LTD ACN 056 783 852
Seventeenth Respondent	PACNET INTERNET (A) PTY LTD ACN 085 213 690
Eighteenth Respondent	TPG NETWORK PTY LTD ACN 003 064 328
Nineteenth Respondent	FTTB WHOLESALE PTY LTD ACN 087 533 328
Twentieth Respondent	CHARIOT PTY LTD ACN 088 377 860
Twenty First Respondent	SOUL PATTINSON TELECOMMUNICATIONS PTY LIMITED ACN 001 726 192
Twenty Second Respondent	SPT TELECOMMUNICATIONS PTY LIMITED ACN 099 173 770
Twenty Third Respondent	SPTCOM PTY LIMITED ACN 111 578 897
Twenty Fourth Respondent	SOUL COMMUNICATIONS PTY LTD ACN 085 089 970
Twenty Fifth Respondent	PIPE NETWORKS PTY LIMITED ACN 099 104 122
Twenty Sixth Respondent	INTRAPOWER TERRESTRIAL PTY LTD ACN 081 193 259
Twenty Seventh Respondent	INTERNODE PTY LTD ABN 82 052 008 581
Twenty Eighth Respondent	TRANSACT CAPITAL COMMUNICATIONS PTY LTD ACN 093 966 888
Twenty Ninth Respondent	TRANSACT VICTORIA COMMUNICATIONS PTY LTD ACN 063 024 475
Thirtieth Respondent	WESTNET PTY LTD ACN 086 416 908
Thirty First Respondent	ADAM INTERNET PTY LTD ACN 055 495 853
Thirty Second Respondent	AAPT LIMITED ACN 052 082 416
Thirty Third Respondent	REQUEST BROADBAND PTY LTD ACN 091 530 586

Appendix A

A. The Pirate Bay

	Domain name	IP address	URL
1.	thepiratebay.se	141.101.118.194,141.101.118.195	https://thepiratebay.se/
2.	bayproxy.pw	104.27.167.96,104.27.166.96	https://bayproxy.pw/
3.	downloadbay.eu	104.28.1.53,104.28.0.53	http://downloadbay.eu/
4.	fastpiratebay.co.uk	104.27.174.252,104.27.175.252	https://fastpiratebay.co.uk/
5.	fastpiratebay.eu	104.28.26.119,104.28.27.119	https://fastpiratebay.eu/
6.	magnetsearch.org	104.24.122.173,104.24.123.173	https://magnetsearch.org/
7.	mypirateproxy.com	104.28.20.2,104.28.21.2	http://mypirateproxy.com/
8.	pirate.guru	104.28.17.148,104.28.16.148	https://pirate.guru/
9.	pirateahoy.eu	104.28.30.50,104.28.31.50	https://pirateahoy.eu/
10.	piratebay.host	198.41.249.68,162.159.240.69	https://piratebay.host/
11.	piratebaymirror.eu	104.28.2.19,104.28.3.19	https://piratebaymirror.eu/
12.	piratebayproxy.be	104.24.118.137,104.24.119.137	http://piratebayproxy.be/
13.	piratebays.co	104.27.168.249,104.27.169.249	https://piratebays.co/
14.	piratebays.co.uk	104.31.76.114,104.31.77.114	https://piratebays.co.uk/
15.	pirateproxy.ca	104.28.2.122,104.28.3.122	http://pirateproxy.ca/
16.	pirateproxy.tf	104.25.209.20,104.25.208.20	https://pirateproxy.tf/
17.	pirateproxy.wf	104.28.4.182,104.28.5.182	https://pirateproxy.wf/
18.	pirateproxy.yt	104.27.138.238,104.27.139.238	https://pirateproxy.yt/
19.	thebay.tv	104.28.6.185,104.28.7.185	https://thebay.tv/
20.	thepiratebay.am	198.105.254.11	https://thepiratebay.am/
21.	thepiratebay.casa	104.27.154.76,104.27.155.76	http://thepiratebay.casa/
22.	thepiratebay.cd	104.31.76.84,104.31.77.84	http://thepiratebay.cd/
23.	thepiratebay.cr	104.28.4.236,104.28.5.236	https://thepiratebay.cr/
24.	thepiratebay.expert	104.18.32.141,104.18.33.141	https://thepiratebay.expert/
25.	thepiratebay.gd	104.24.100.99	https://thepiratebay.gd/
26.	thepiratebay.gs	104.24.99.150	
27.	thepiratebay.la	104.28.2.115	http://thepiratebay.la/

	Domain name	IP address	URL
28.	thepiratebay.mn	104.27.156.189	http://thepiratebay.mn/
29.	thepiratebay.org	104.18.40.167,104.18.41.167	http://thepiratebay.org/
30.	thepiratebay.uk.net	104.18.58.238,104.18.59.238	https://thepiratebay.uk.net/
31.	thepiratebay.vg	104.28.4.121	http://thepiratebay.vg/
32.	thepiratebay.xn--fiqs8s	104.28.2.96,104.28.3.96	http://thepiratebay.xn--fiqs8s/
33.	thepiratebay.xn--q9jyb4c	104.27.144.26,104.27.145.26	http://thepiratebay.xn--q9jyb4c/
34.	thepiratebay-proxy.com	104.28.10.55,104.28.11.55	https://thepiratebay-proxy.com/
35.	thepirateboat.eu	104.28.6.62,104.28.7.62	https://thepirateboat.eu/
36.	tpbmirror.us	104.28.7.41,104.28.6.41	https://tpbmirror.us/
37.	urbanproxy.eu	104.28.13.69,104.28.12.69	https://urbanproxy.eu/

B. Torrentz

	Domain name	IP address	URL
1.	torrentz.eu	185.87.144.3,185.87.144.4,185.87.147.3,185.87.147.4	http://torrentz.eu/
2.	torrentsmirror.com	104.28.29.56,104.28.28.56	http://torrentsmirror.com/
3.	torrentz.ch	185.87.144.3,185.87.144.4,185.87.147.3,185.87.147.4	http://torrentz.ch/
4.	torrentz.com	72.52.4.119	http://torrentz.com/
5.	torrentz.hk	185.87.147.4,185.87.144.3,185.87.144.4,185.87.147.3	http://torrentz.hk/
6.	torrentz.in	185.87.147.3,185.87.147.4,185.87.144.3,185.87.144.4	http://torrentz.in/
7.	torrentz.li	185.87.147.4,185.87.144.3,185.87.144.4,185.87.147.3	http://torrentz.li/
8.	torrentz.me	185.87.144.3,185.87.144.4,185.87.147.3,185.87.147.4	http://torrentz.me/
9.	torrentz.ph	185.87.147.4,185.87.144.3,185.87.144.4,185.87.147.3	http://torrentz.ph/

	Domain name	IP address	URL
10.	torrentz-proxy.com	185.87.144.3, 185.87.144.4, 185.87.147.3, 185.87.147.4	http://torrentz-proxy.com/
11.	tz.ai	185.87.144.3, 185.87.144.4, 185.87.147.3, 185.87.147.4	http://tz.ai/

C. TorrentHound

	Domain name	IP address	URL
1.	torrenthound.com	88.80.6.5	http://www.torrenthound.com/
2.	torrenthound.at	104.31.88.28, 104.31.89.28	http://torrenthound.at/
3.	torrenthound.cm	104.31.80.128, 104.31.81.128	http://torrenthound.cm/
4.	torrenthound.immunity.info	104.28.2.124, 104.28.3.124	https://torrenthound.immunity.info/
5.	torrenthound.ru	104.24.100.232, 104.24.101.232	http://torrenthound.ru/
6.	torrenthound.to	88.196.31.41	http://torrenthound.to/
7.	torrenthound.unlocktor.eu	5.45.77.184	http://torrenthound.unlocktor.eu/
8.	torrenthound-proxy.com	104.18.58.145, 104.18.59.145	http://torrenthound-proxy.com/

D. IsoHunt

	Domain name	IP address	URL
1.	isohunt.to	198.41.189.233, 198.41.190.233	https://isohunt.to/
2.	isohunt.duhsoft.com	5.45.75.223	http://isohunt.duhsoft.com/
3.	isohunt.kooaba.net	5.45.64.109	http://isohunt.kooaba.net/
4.	isohunt.st	173.236.194.74	http://www.isohunt.st/
5.	isohunters.net	78.142.19.12	http://isohunters.net/