IN THE HIGH COURT OF AUSTRALIA
SYDNEY REGISTRY

No. S288 of 2011

BETWEEN:

ROADSHOW FILMS PTY LTD (ACN 100 746 870) AND THE OTHER PARTIES IN SCHEDULE 1
Appellant

and

IINET LIMITED (ACN 068 628 937)
Respondent

INTERVENER'S SUBMISSIONS BY THE AUSTRALIAN PRIVACY FOUNDATION ON APPLICATION TO BE HEARD AS *AMICUS CURIAE*, AND IF LEAVE IS GRANTED, ON THE APPEAL

Part I: Suitable for publication

1. The Australian Privacy Foundation ("APF") certifies that this submission is in a form suitable for publication on the Internet.

Part II: Basis of intervention

2. The APF seeks leave to be heard as *amicus curiae* in this matter.

3. The APF is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. Since 1986, the Foundation has been the principal non-government organisation (NGO) defending the right of individuals to control their personal information and to be free of excessive intrusions.

4. The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

5. The APF is an entirely independent organisation.

6. When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, privacy oversight agencies, professional associations and other community groups as

Australian Privacy Foundation
607/70 Remembrance Dr,
SURFERS PARADISE QLD 4217

Telephone: (07) 5595 1418
Fax: (07) 5595 1011
Ref: Dr Dan Svantesson

6 October 2011

appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

7. The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

8. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

9. The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law. The work of the APF is further assisted by its Patron and Advisory Panel consisting of leading citizens.[1]

10. The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. At the same time, the fact that online privacy is a major concern to the Australian public seems beyond intelligent dispute, and is backed up by ample statistical evidence. For example already in 2001, responses to research on community attitudes to privacy, conducted by the Office of the Privacy Commission, showed that 90% of Internet users viewed monitoring of their Internet usage without consent as privacy invasive.[2]

Part III: Why leave should be granted

11. The matter of the appeal is set in the area of copyright law. However,he issue of what responsibility Internet Service Providers ("ISPs") should bear in relation to alleged copyright infringements raises questions of general public importance.

12. Privacy is a major issue as the activities of both the appellants and the respondent involve the collection, use and disclosure of personal information. Neither the collection of evidence by the appellants, nor the activities the appellants want the respondent to engage in, can take place without invasions of the privacy of individual Internet users. Consequently, any answer the Court gives as to the correct interpretation of s. 101(1A) of the *Copyright Act 1968* (Cth), and more broadly to the question of the level of knowledge required for a finding of authorisation of copyright infringement, will affect the privacy of virtually every Australian on a day to day basis.

---

[1] http://www.privacy.org.au/About/AdvisoryPanel.html.

[2] Submission by the Office of the Federal Privacy Commissioner to the Copyright Digital Agenda Review: Carriers and Carriage Service Providers Issues Paper (October 2003), at 4. http://www.privacy.gov.au/materials/types/submissions?filterby=2003&sortby=65.

13. If the Court is minded to grant leave, we seek only to rely on our written submissions. We do not seek leave to present oral submissions.

14. The APF's submissions aim to bring attention to the significant privacy considerations that impact upon the questions raised in the appeal.

15. So as to not inconvenience the proceedings, the submissions do not seek to raise any additional legal issues. They present additional arguments on legal issues the Court will address within the appeal and do not overlap with the arguments raised by the parties (or the interveners). Thus, should leave be granted, the APF's submissions should not add any materially additional costs. Nor should they materially affect the duration of the proceedings.

16. Finally, as is clearly demonstrated by the fact that privacy has gained no attention in the proceedings to date, the APF's interest in the matter is distinct from those of the parties. It appears that, but for the APF's submissions, those privacy interests will be overlooked, or at least, be given insufficient emphasis.

Part IV: Applicable provisions and regulations

17. Apart from the statutory provisions of the *Privacy Act 1988* (Cth) referred to in this submission, the appellant's submission dated 9 September 2011 contains (as Annexure "A") the relevant statutory provisions as they existed at the relevant time, and at present. Annexure "A" of the APF's submission contains the relevant statutory provisions of the *Privacy Act 1988* (Cth).

Part V: Submissions

18. While ascertaining the correct meaning of s. 101(1A) of the *Copyright Act 1968* (Cth) is a matter of legal interpretation, the Court must, it is submitted, be mindful of the societal implications that flow from the interpretation it chooses to favour. The impact the decision has on the day to day privacy of the Australian public is at the heart of those implications. This is particularly serious as important aspects of societal interaction takes place online and Australians live an increasingly large part of their life through the Internet.

The privacy framework

19. Privacy is recognised as a fundamental human right in a number of important international agreements. For example, Article 17 of the International Covenant on Civil and Political Rights (New York, 16 December 1966), to which Australia is a party, reads as follows:

> *1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
>
> *2. Everyone has the right to the protection of the law against such interference or attacks.*

20. In addition, privacy rights are protected through a patchwork of state and federal legislation in Australia, most notably, the *Privacy Act 1988* (Cth). Importantly, that Act includes 10 National Privacy Principles that apply to the parties in this matter. Furthermore, the extent to which privacy interests are protected under Australian law by either or both of a tort of interference with privacy, or the law of breach of confidence, has not yet been fully determined by Australian courts. Both types of actions are still possible sources of protection for the privacy of Australians.

21. Thus, it is the APF's submission that, privacy is of relevance here, both as directly and clearly prescribed legal rules under the relevant law, and as a more broadly defined fundamental human right.

How privacy fits within *Copyright Act 1968* (Cth) s. 101(1A)

22. The APF submits that, while not expressly mentioned, privacy considerations play a central role in the correct interpretation of s. 101(1A), which includes three elements that must be taken into account when determining whether a person has authorised a copyright infringement:

> *(a) the extent (if any) of the person's power to prevent the doing of the act concerned;*
>
> *(b) the nature of any relationship existing between the person and the person who did the act concerned;*
>
> *(c) whether the person took any other reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice.*

23. It is the APF's submission that, privacy considerations arise in relation to all of these elements. In speaking of "*whether the person took any other reasonable steps to prevent or avoid the doing of the act*", s. 101(1A)(c) makes clear that such a person cannot be expected to do all that lies within its power. Rather the taking of reasonable steps suffices. Furthermore, a person could not be expected to take steps which would otherwise be in breach of the law, whether statutory rights of privacy or privacy protections arising otherwise in law or equity.

24. In assessing what steps reasonably can be taken by an ISP faced with evidence suggesting that some of its customers, or persons using the connection of its customers, have engaged in copyright infringements, several interests must be balanced against each other, and account must be taken of the ISP's privacy obligations to both its customers and to other persons using the connection of its customers. Put differently, whether it actually violates privacy law or not, a step is not reasonable if it involves a disproportionate interference with the customer's, or another person's, privacy.

25. In this context, it must be kept in mind that, the option of pursuing their interests through established court procedures remains open to the Copyright Owners. The existence of such an alternative, with the safeguards it entails,

undermines any suggestion that drastic routine invasions of privacy are justifiable by reference to the financial interest of the Copyright Owners.

26. Indeed, without condoning, or excusing, copyright infringements, one may, from a policy point of view argue that, the steps Copyright Owners can take to adjust their business models, so as to discourage copyright infringements, ought to be considered when assessing what steps they reasonably can expect an ISP to take on their behalf.

27. In any matter similar to that at hand, the ISP's "*power to prevent the doing of the act concerned*" (referred to in s. 101(1A)(a)) is limited by the fact that it has an obligation to comply e.g. with the *Privacy Act 1988* (Cth), the *Telecommunications Act 1997* (Cth), any other statutory provisions, and any protections of privacy provided through common law or equity.

28. Apart from observing that it may be that the matter deserves closer attention than has been provided so far, these submissions will not address the legal issues that arise in relation to the *Telecommunications Act 1997* (Cth).

29. It is, however, the APF's submission that, regardless of how the Court determines the correct application of the *Telecommunications Act 1997* (Cth), the *Privacy Act 1988* (Cth) imposes important restrictions on how an ISP may collect[3], use and disclose[4] personal information about its customers, and about its non-customer users.

30. When examining "*the nature of any relationship existing between the person and the person who did the act concerned*" it must be remembered that, that relationship will always have a privacy dimension to it; it will always impose certain privacy obligation (e.g. stemming from the *Privacy Act 1988* (Cth) or the law of breach of confidence), on the ISP. Those privacy obligations must necessarily impact on the application of s. 101(1A).

31. Further, due to the common practise of several persons (e.g. a family) sharing the same Internet connection, in a significant number of cases, the ISP's customer will not be the actual infringer. For the ISP to be liable for having authorised the infringement, it would be necessary to argue that the customer is liable for authorising the actual infringer's act. It would then be necessary to argue that the ISP in some sense is liable for the customer's authorisation. This means that in such a case, the position of the ISP is rather disconnected from the actual infringement.

32. In such a case, the ISP's "*power to prevent the doing of the act concerned*" (referred to in s. 101(1A)(a)) is limited by the fact that, preventing the infringement can only be done by cutting the Internet connection to the actual customer; a person who has not engaged in the actual copyright infringement. At a minimum, this brings attention to the fact that iiNet may be dealing with the

---

[3] National Privacy Principle 1.

[4] National Privacy Principle 2.

personal information of third parties with whom it has no contractual arrangement. The importance of this is elaborated upon below.

The types of personal information in question

33. The appellant's submission ([14]) provides a useful list of the types of information it, or parties acting on its behalf, have collected and used:

> *"PeerID", date and time, file name downloaded, hash, filmfTV title, studio, percentage of file shared, MB [megabytes] downloaded, percentage of file downloaded, peer host name and country.*

10

34. Further guidance as to the extent of the collection can be gained, e.g., from Emmett J's discussion:[5]

> *DtecNet Agent created a running log of every activity, which included every single request sent between computers and every packet of data exchanged between those computers. Accordingly, every aspect of the connection and download was recorded and logged by DtecNet Agent. All the information received by DtecNet Agent was recorded and stored on DtecNet's servers.*

20 35. The information iiNet would need to use to warn, or to suspend or terminate provision of services to, a customer plainly fall within the classification of personal information:[6]

a) *The IP addresses and times and other information provided by the infringement notices (AFACT information).*

b) *Information identifying the IP addresses that were allocated to particular iiNet customers at particular times (score information).*

c) *Information as to the personal details, such as names, addresses, email addresses and telephone numbers, of iiNet's customers (rumba information).*

30 36. Thus, it must be common ground that, in the hands of the ISP, this information identifies an individual and therefore amount to the type of 'personal information' protected under the *Privacy Act 1988* (Cth):[7]

> *"personal information" means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*

---

[5] (2011) 275 ALR 1 at 17 [69].

[6] (2011) 275 ALR 1 at 52 [230].

[7] *Privacy Act 1988* (Cth), s. 6.

37. However, the *AFACT information* alone, may amount to personal information. The literature, and court decisions, on whether an IP address amounts to personal information is too voluminous to be given justice here. Importantly, the Australian Law Reform Commission has expressed the following view:[8]

> *While stand alone telephone numbers, street addresses and IP addresses may not be personal information for the purposes of the Privacy Act, such information may become personal information in certain circumstances. The ALRC acknowledges that telephone numbers relate to telephones or other communications devices, IP addresses to computers, and street addresses to houses, rather than individuals, but notes that such information may come to be associated with a particular individual as information accretes around the number or address.*

38. In commenting on this issue, the influential EU Advisory Body on Data Protection and Privacy (the Article 29 Working Group) goes even further, and has taken the view that: *"IP addresses attributed to Internet users are personal data and are protected by EU Directives 95/46 and 97/66."*[9] The Working Party reached its conclusion in light of the fact that *"[i]n the case of IP addresses the ISP is always able to make a link between the user identity and the IP addresses and so may be other parties, for instance by making use of available registers of allocated IP addresses or by using other existing technical means."*[10]

39. Thus, whether the information collected by the Copyright owners, or on their behalf, amounts to personal information must be assessed in each individual case. An assessment also needs to be made whether any obligations of confidence attach to the information.

40. The types of information discussed above may appear of limited significance at a first glance. However, upon reflection it is clear that such data can reveal important facts about a person (or group of persons) such as interests, philosophical beliefs, political opinions, and sexual preferences or practices. Thus, in a privacy sense, this is sensitive personal information as defined in s. 6 of the *Privacy Act 1988* (Cth) afforded special protection under National Privacy Principle 10. Further, such information may also reveal facts about the person's (or group of persons') habits, such as when they use their computers, which in turn can be used to ascertain when the person (or group of persons) spend time at home, and can e.g. be targeted for marketing calls and the like. The realisation that such information is of importance is well illustrated in the current debate about the use of smart metering of energy consumption (see further Rainer Knyrim and Gerald Trieb, Smart metering under EU data protection law, *International Data Privacy Law* (2011) 1(2): 121-128).

---

[8] AUSTRALIAN LAW REFORM COMMISSION, FOR YOUR INFORMATION: AUSTRALIAN PRIVACY LAW AND PRACTICE ¶ 6.60 (Report No. 108, 2008).

[9] Article 29 Data Protection Working Party, *Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6*, WP 58, at 3 (adopted on May. 30, 2002), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp58_en.pdf.

[10] *Id.*

41. Attention should also be given to the type of information an ISP would be required to provide to a customer it is alleging has violated the terms of service by infringing copyright. One would think that fairness demands that such an allegation, particularly if coupled with a threat of terminating the service, or an actual termination of the service, would need to include details of the allegation, such as when the alleged infringement would have occurred and the nature of the alleged infringement. The problem this gives rise to is that, as concluded above, in a significant number of cases, the actual infringer will not be the ISP's customer. In such cases, the ISP is likely to be disclosing personal information about the alleged infringer to the customer. Such a disclosure would be particularly serious where the allegation is based on inaccurate data.

Selected privacy issues

42. Apart from the privacy issues already introduced, the APF submits that, there are several other privacy concerns that must impact upon the correct interpretation of s. 101(1A).

43. First, any large collection of personal information is a concern. As demonstrated time and time again, such collections work as 'honey pot' for hackers seeking personal information e.g. to be used for identity crime. One need not look far to find examples. As recently as May 2011, it was reported that a private company (TMG) that scans file-sharing networks and gathers the IP addresses of alleged infringers as part of the French government's 'three strikes' approach to online copyright infringement suffered an embarrassing security breach forcing the French government to *"temporarily suspend"* its acquisition of new data from TMG.[11]

44. Importantly, the Office of the Privacy Commissioner has told a Senate Standing Committee that:[12]

> *Broad scale collection and retention of web browsing information could significantly impact on the privacy of individuals. Possible privacy issues could include greater risks of data loss or misuse, unwarranted surveillance, data linking and data mining, and identity theft.*

45. In this context, it is also relevant to consider the Office of the Privacy Commissioner's position that:[13]

> *In the Office's view, any collection and use of personal information for law enforcement purposes should be:*

---

[11] Ars Technica - "France halts 'three strikes' IP address collection after data leak" http://arstechnica.com/tech-policy/news/2011/05/france-halts-three-strikes-ip-address-collection-after-data-leak.ars.

[12] The adequacy of protections for the privacy of Australians online - Submission to Senate Standing Committee on Environment, Communications and the Arts (August 2010) http://www.privacy.gov.au/materials/types/download/9558/7122.

[13] *Id.*

- *a necessary response to a clearly defined problem*
- *proportionate to the risk posed*
- *subject to a privacy impact assessment, and*
- *accompanied by adequate accountability and review mechanisms.*

46. There can be no doubt that an even more stringent standard is justified where the collection and use is by private entities for the enforcement of private property rights.

47. In 2003, the Office of the Federal Privacy Commissioner considered in detail a streamlined process for obtaining access to ISP subscriber details, especially in response to alleged breaches of copyright. The key recommendations/opinions from this submission were:[14]

a) The least privacy intrusive alternative process should be considered with respect to any streamlined process for access to ISP subscriber details.

b) Any access regime which might invest in private sector industries or interests, powers to access subscriber information in a way which is currently possible only through law enforcement agencies and to further infringe on the privacy of subscribers to ISP services in order to address copyright infringement concerns is opposed.

c) The implementation of any streamlined process should provide stringent, privacy and legal protections equivalent to the current mechanisms in place to protect access to ISP subscriber information, and not diminish existing protections around disclosure of subscriber information.

i) For example, a process along similar lines to that adopted under the Digital Millennium Copyright Act (1998) in the United States is likely to be inconsistent with existing privacy protections in the Telecommunications and Privacy Acts:

> *It is not clear from the Issues paper how, in a more streamlined process, the authority to investigate infringements of copyright would be invested or in whom. The high level of privacy invasiveness of the activity would demand a commensurate level of authority to govern decisions on access. At present, the power is vested in the courts to rule on discovery applications and on appropriate judicial authorities to issue warrants to law enforcement agencies investigating potential criminal breaches of copyright.*
> *Any new processes to permit access to subscriber information should include stringent rules to limit access to cases that are serious and where there are significant grounds for suspecting a breach. For example, it may not be appropriate to allow personal*

[14] Submission by the Office of the Federal Privacy Commissioner to the Copyright Digital Agenda Review: Carriers and Carriage Service Providers Issues Paper (October 2003), http://www.privacy.gov.au/materials/types/download/8640/6486.

information collected by law enforcement agencies under warrant in the course of a criminal investigation to be subsequently used for civil actions.[15]

ii) Attempts to overcome privacy obligations by inducing individual subscribers to 'sign away' privacy protections and submit to increasingly privacy-intrusive 'bundled-consent' processes in order to access ISP services or internet information are of concern.

48. There is also reason to take account of the regulation of transborder data flows. Indeed, in the matter at hand the evidence of the infringements was collected by technicians operating partly in Australia and partly in Northern and Eastern Europe. It can, thus, be assumed that information about the online activities of Australians may find its way to foreign countries, perhaps with weaker privacy protection than what is provided in Australia. Under National Privacy Principle 9 such cross-border data transfer is a key issue in privacy law.

49. To all this, it may be objected that the customer consents to the use and disclosure of its personal information. Indeed, as discussed by Emmett J ([245]), an argument along those lines was presented by the appellants in the context of s. 289 of the *Telecommunications Act 1997* (Cth). However, such an objection evaporates in a sober-minded consideration of the real state of things.

50. First, while the customers consent to the collection and use of their personal information so that iiNet can provide them with its services, there is nothing to suggest they automatically also consent to that information being used by iiNet to monitor their compliance with copyright laws, on behalf of domestic and overseas Copyright Owners. Such consent is not express and cannot be implied as the customer cannot be viewed as having been sufficiently informed. Indeed, the provision of the service, and iiNet monitoring compliance with copyright laws, being distinct matters, it would be inappropriate for the customer's consent on those two matter being bundled together:[16]

> *The Federal Privacy Commissioner has expressed concerns about the practice of 'bundling consent', that is, making delivery of a service conditional upon the individual giving consent for other forms of information handling practice that are not necessary for delivery of the service. This is particularly of concern where the practice would otherwise fall outside of the allowable uses and disclosures of personal information under the Privacy Act.*

51. Second, as noted, the proposed actions to be taken by iiNet may disclose personal information about third persons to iiNet's customers. Those third

---

[15] Submission by the Office of the Federal Privacy Commissioner to the Copyright Digital Agenda Review: Carriers and Carriage Service Providers Issues Paper (October 2003), at 4 http://www.privacy.gov.au/materials/types/download/8640/6486.

[16] *Id.*

persons have not entered into any contractual relationship with iiNet and are, thus, unlikely to have provided consent.

52. A Court ruling favouring the appellants will doubtlessly encourage further, potentially more extensive and intrusive, data collection and use by Copyright Owners and other private organisations acting on their behalf. It is hard to imagine how the Australian public's legitimate privacy interests will be catered for in case of such a development.

Correct application of *Moorhouse*[17] and s. 101(1A)

53. The standard applied in determining when an ISP must act where a rights holder brings attention to an alleged infringement will inevitably have privacy implications. Put simply, the lower that standard is set, the greater the privacy risks.

54. The appellants have identified an area of uncertainty in pointing to the fact that, s. 101(1A) does not provide any guidance as to the level of knowledge that is required for a party being found to have authorised an infringement. They contend that Emmett J and Nicholas J both erred in conflating the question of the requisite degree of knowledge and the question of what steps iiNet reasonably could take.

55. It is the APF's submission that neither the honourable Emmett J, nor the honourable Nicholas J, erred in this regard. In fact, the APF submits that the question of the requisite degree of knowledge and the question of what steps an ISP reasonably can take, are intimately connected and that, on a careful reading, there is nothing in *Moorhouse* that stands in the way of the approaches adopted by Emmett J and Nicholas J in this regard.

56. Plainly, a high degree of knowledge of the primary infringement is required where the steps taken involve highly intrusive acts such as the suspension or termination of a customer's Internet access. In contrast, where the step to be taken is merely the placing of a copyright notice at an appropriate location, a lower degree of knowledge of the primary infringement may be required.

57. If these submissions are accepted, there is nothing in the appellants' arguments that stands in the way of a more privacy-friendly solution being found.

58. Taking account of the principles established in *Moorhouse*, and having regard to the wording of s. 101(1A), the APF submits that it is open to the Court to conclude that an ISP can be asked to do no more to discourage copyright infringements than what iiNet already is doing.

59. It is the APF's submission that, if, in order to avoid being held to have authorised copyright infringements, an ISP is required to take further steps where provided with adequate evidence to give it actual knowledge of a specific infringement, it could only be required to send the relevant customer a

---

[17] *University of New South Wales v Moorhouse* (1975) 133 CLR 1.

reminder of its obligations in relation to copyright. To avoid being privacy invasive, and to avoid adding materially to the ISP's costs, such a reminder should be generic. An ISP cannot reasonably be required to take any other steps until the infringement has been proved in a court or admitted by the relevant customer.

60. Finally on this issue, in their submissions, the appellants point to the fact that iiNet, from time to time, *"suspended or terminated subscriber's accounts on the basis of non-payment of fees"* ([8]). The relevance of this, in determining what reasonable steps iiNet should take in response to the alleged copyright infringements, is limited. Proving the non-payment of fees involves no third-party collection and use of the customer's personal information. Nor does it involve the potential disclosure of third-party personal information, by the ISP to the customer, as would be the case where the infringement was carried out by somebody other than the customer.

The honourable Emmett J's test

61. The honourable Emmett J articulated a test for determining when it *"would be reasonable for iiNet to take steps within the meaning of s 101(1A)(c) to suspend or terminate a customer's account"* ([210]). In that test, focus is essentially placed on:

(a) iiNet having been *"provided with unequivocal and cogent evidence of the alleged primary acts of infringement by use of the iiNet service in question"*;

(b) the customer having received sufficient notice and having had adequate possibilities for disputing the claim; and

(c) the Copyright Owners having undertaken:

> *to reimburse iiNet for the reasonable cost of verifying the particulars of the primary acts of infringement alleged and of establishing and maintaining a regime to monitor the use of the iiNet service to determine whether further acts of infringements occur, and to indemnify iiNet in respect of any liability reasonably incurred by iiNet as a consequence of mistakenly suspending or terminating a service on the basis of allegations made by the copyright owner.*

62. Should the Court embrace this test, it is respectfully submitted that at least two additional elements should be added. First, the Copyright Owners should also be required to show that they have undertaken an adequate Privacy Impact Assessment ("PIA") in relation to their method of collecting the evidence. A guide which should assist the Copyright Owners in meeting this obligation was published in 2010 by the Office of the Privacy Commissioner, and further guidance can be gained e.g. from Dr Roger Clarke's article "An evaluation of privacy impact assessment guidance documents" (International Data Privacy Law (2011) 1(2): 111-120)).

63. The reasonableness of ISPs requesting evidence of a PIA is apparent from the fact that the ISP will be deemed to have collected the personal information ...

provided by the Copyright Owners and will have a responsibility under the *Privacy Act 1988* (Cth) to ensure its accuracy (National Privacy Principle 3), and as well that collection was *"by lawful and fair means and not in an unreasonably intrusive way"* (National Privacy Principle 1.2).

64. Second, the honourable Emmett J's test clearly anticipates claims being made against the ISPs by aggrieved customers wrongly accused of infringements. In that context, account must be had of the emerging statutory right of action for privacy violations (and/or the emerging tortious right of action for intrusion of privacy or breach of confidence previously envisaged by this Court in ABC v Lenah Game Meats (2001) 185 ALR 1).[18] It does not require any great deal of imagination to foresee such actions (possibly coupled with claims of defamation) being taken against an ISP who acts on a flawed infringement notice.

65. While there can be no doubt an aggrieved customers wrongly accused of infringements must have a right to take action against the ISP, it would seem more efficient for such claims to be allowed to also be made directly against the Copyright Owners as the source of the flawed allegations.

Conclusions

66. Ultimately, it is the APF's submission that ISPs are poorly placed to assume the role that the Copyright Owners wish to impose upon them. As recently noted by the Organisation for Economic Co-operation and Development ("OECD"): *"A critical role of Internet intermediaries is to establish trust, including through protection of user privacy."*[19] Procedural fairness, and the need to minimise the risk of e.g. privacy abuse, requires the party assessing whether or not a person has engaged in copyright infringements to be a disinterested party in the matters it deals with. This is particularly so were a finding of guilt may result in the offender effectively being cut off from key aspects of society by being unable to gain Internet access.

67. There is no reason to assume that the Australian public trusts their ISPs to act as judge and jury, determining whether they have infringed copyright. After all, it would be absurd to suggest that ISPs are disinterested parties in such inquiries if they can be held to have authorised the infringement if they fail to find an offender guilty. No one would accept a legal system where judges who failed to convict an offender had to carry the sentence in the offender's place. And a system that does not contain sufficient procedural fairness in the hands of trained judges could hardly be appropriate in the hands of an organisation in the private sector.

68. Under the system sought by the appellants, ISPs would be likely to err on the side of caution so as to avoid the risk of being held to have authorised copyright infringements. Thus, it cannot be expected that privacy

---

[18] Commonwealth Government's issues paper, *A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy* (23 September 2011) http://www.dpmc.gov.au/privacy/causeofaction/.
[19] Organisation for Economic Co-operation and Development, The economic and social role of internet intermediaries (April 2010), at 8 http://www.oecd.org/dataoecd/49/4/44949023.pdf.

considerations, and other matters such as procedural fairness, would be given due weight in the ISPs' inquiry into the guilt of their customers.

69. The appellants seek to fundamentally change the nature of the relationship of the ISP (and their professional engineering staff) to their customer, from one who is simply paid to provide services and otherwise act in the customer's interests, to a relationship where, under threat of imposition of liability for infringement of the commercial rights of would-be litigants largely based outside the jurisdiction, the ISP is still paid and provides services, but in addition also provides unpaid surveillance and/or evidence collection services for those foreign litigants and acts against the interests of the customer upon allegations made by the foreign litigants, who chooses not to pursue legal remedies open to it that would test the evidence and law in a court. Such a fundamental and punitive change in the role of the ISP as intermediary should not be contemplated without consideration of all factors affecting reasonableness and necessity, including alternative options at each point in the argument.

70. Our submissions have sought to highlight that the Court's decision as to the matters of the appeal will impact on the day to day privacy of virtually every person in Australia. While it would seem eccentric to deny that the Copyright Owners have a legitimate claim to pursue their financial interest, it must be remembered that those financial interest cannot be given greater weight than the interest of upholding an adequate level of protection for the fundamental human right to be shielded from privacy violations.

71. With the Internet being a near perfect tool for surveillance and monitoring, privacy must be tended with care in every decision that impacts upon it, if our fundamental human right of privacy is to be preserved in modern society.

Dated 6 October 2011

Name: Dr Dan Svantesson,
Vice-Chair, Australian Privacy Foundation
Telephone: (07) 5595 1418
Facsimile: (07) 5595 1011
Email: vicechair2@privacy.org.au

ANNEXURE A

Relevant statutory provisions

Privacy Act 1988 (Cth)

6 Interpretation

personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

sensitive information means:

(a) information or an opinion about an individual's:
  (i) racial or ethnic origin; or
  (ii) political opinions; or
  (iii) membership of a political association; or
  (iv) religious beliefs or affiliations; or
  (v) philosophical beliefs; or
  (vi) membership of a professional or trade association; or
  (vii) membership of a trade union; or
  (viii) sexual preferences or practices; or
  (ix) criminal record;
  that is also personal information; or
(b) health information about an individual; or
(c) genetic information about an individual that is not otherwise health information.

National Privacy Principle 1 – Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:
  (a) the identity of the organisation and how to contact it; and
  (b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and
(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
(e) any law that requires the particular information to be collected; and
(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

National Privacy Principle 2 – Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless:
(a) both of the following apply:
(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or
(b) the individual has consented to the use or disclosure; or
(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
(i) it is impracticable for the organisation to seek the individual's consent before that particular use; and
(ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
(iii) the individual has not made a request to the organisation not to receive direct marketing communications; and
(iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and
(v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or

other electronic means, a number or address at which the organisation can be directly contacted electronically; or

(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or

(ii) a serious threat to public health or public safety; or

(ea) if the information is genetic information and the organisation has obtained the genetic information in the course of providing a health service to the individual:

(i) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of an individual who is a genetic relative of the individual to whom the genetic information relates; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95AA for the purposes of this subparagraph; and

(iii) in the case of disclosure—the recipient of the genetic information is a genetic relative of the individual; or

(f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) the individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the ***carer***) providing the health service for the organisation is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(c) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is ***responsible*** for an individual if the person is:

(a) a parent of the individual; or
(b) a child or sibling of the individual and at least 18 years old; or
(c) a spouse or de facto partner of the individual; or
(d) a relative of the individual, at least 18 years old and a member of the individual's household; or
(e) a guardian of the individual; or
(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or
(g) a person who has an intimate personal relationship with the individual; or
(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

child: without limiting who is a child of an individual for the purposes of this clause, each of the following is the ***child*** of an individual:
(a) an adopted child, stepchild, exnuptial child or foster child of the individual; and
(b) someone who is a child of the individual within the meaning of the *Family Law Act 1975*.

de facto partner has the meaning given by the *Acts Interpretation Act 1901*.

parent: without limiting who is a parent of an individual for the purposes of this clause, someone is the ***parent*** of an individual if the individual is his or her child because of the definition of ***child*** in this subclause.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

stepchild: without limiting who is a stepchild of an individual for the purposes of this clause, someone is the ***stepchild*** of an individual if he or she would be the individual's stepchild except that the individual is not legally married to the individual's de facto partner.

2.7 For the purposes of the definition of ***relative*** in subclause 2.6, relationships to an individual may also be traced to or through another individual who is:
(a) a de facto partner of the first individual; or
(b) the child of the first individual because of the definition of ***child*** in that subclause.

2.8 For the purposes of the definition of ***sibling*** in subclause 2.6, an individual is also a sibling of another individual if a relationship referred

to in that definition can be traced through a parent of either or both of them.

National Privacy Principle 3 – Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

National Privacy Principle 9 – Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

National Privacy Principle 10 – Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected:

(i) as required or authorised by or under law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection; and

(d) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

SCHEDULE 1

SECOND TO THIRTY-FOURTH APPELLANTS

UNIVERSAL CITY STUDIOS LLP

Second Applicant

PARAMOUNT PICTURES CORPORATION

Third Applicant

WARNER BROS. ENTERTAINMENT INC

Fourth Applicant

DISNEY ENTERPRISES, INC

Fifth Applicant

COLUMBIA PICTURES INDUSTRIES, INC

Sixth Applicant

TWENTIETH CENTURY FOX FILM CORPORATION

Seventh Applicant

PARAMOUNT HOME ENTERTAINMENT (AUSTRALASIA)

Eighth Applicant

BUENA VISTA HOME ENTERTAINMENT, INC.

Ninth Applicant

TWENTIETH CENTURY FOX FILM CORPORATION (AUSTRALIA) PTY LIMITED

Tenth Applicant

UNIVERSAL PICTURES (AUSTRALASIA) PTY LTD

Eleventh Applicant

VILLAGE ROADSHOW FILMS (BVI) LTD

Twelfth Applicant

UNIVERSAL PICTURES INTERNATIONAL B.V

Thirteenth Applicant

UNIVERSAL CITY STUDIOS PRODUCTIONS LLLP

Fourteenth Applicant

RINGERIKE GMBH & CO KG

Fifteenth Applicant

INTERNATIONALE FILMPRODUKTION BLACKBIRD VIERTE GMBH & CO KG

Sixteenth Applicant

MDBF ZWEITE FILMGESELLSCHAFT MBH & CO KG

Seventeenth Applicant

INTERNATIONALE FILMPRODUKTION RICHTER GMBH & CO KG

Eighteenth Applicant

NBC STUDIOS, INC

Nineteenth Applicant

DREAMWORKS FILMS L.L.C.

Twentieth Applicant

WARNER BROS INTERNATIONAL TELEVISION DISTRIBUTION INC
Twenty-first Applicant

TWENTIETH CENTURY FOX HOM ENTERTAINMENT INTERNATIONAL CORPORATION
Twenty-second Applicant

WARNER HOME VIDEO PTY LTD

Twenty-third Applicant

PATALEX III PRODUCTIONS LIMITED

Twenty-fourth Applicant

LONELY FILM PRODUCTIONS GMBH & CO KG
Twenty-fifth Applicant

SONY PICTURES ANIMATION INC

Twenty-sixth Applicant

UNIVERSAL STUDIOS INTERNATIONAL B.V.
Twenty-seventh Applicant

SONY PICTURES HOME ENTERTAINMENT PTY LTD
Twenty-eighth Applicant

GH ONE LLC

Twenty-ninth Applicant

GH THREE LLC
Thirtieth Applicant

BEVERLY BLVD LLC
Thirty-first Applicant

WARNER BROS ENTERTAINMENT AUSTRALIA PTY LTD
Thirty-second Applicant

TWENTIETH CENTURY FOX HOME ENTERTAINMNET LLC
Thirty-third Applicant

SEVEN NETWORK (OPERATIONS) LIMITED
Thirty-fourth Applicant