Submission of the

University of New South Wales Council for Civil Liberties

to the

Attorney-General's 2003 Review of the

Copyright Amendment (Digital Agenda) Act 2001

1 October 2003

Authors: David Leung, University of New South Wales Council for Civil Liberties
Michael Walton, University of New South Wales Council for Civil Liberties

1. Introduction

The University of New South Wales Council for Civil Liberties (UNSWCCL) wishes to address submissions to two issues concerning the liability of carriers and carriage service providers. Specifically UNSWCCL's submissions are made in relation to Issues 15 and 16 of the review:

15. the extent to which Service Providers should be required to provide access to subscriber details. If required to do so, the extent to which the Federal Court Rules are a sufficient mechanism for such an access regime or whether an alternative process is required;[1] and,

16. the privacy and confidentiality implications of an access regime.[2]

While UNSWCCL does not deny that copyright holders may have a legitimate interest in seeking the particulars of infringers, the privacy and confidentiality implications of any access regime must be considered. The existing access regime is that of discovery in accordance with the Federal Court Rules. UNSWCCL is concerned about the operation of, and privacy implications associated with, the procedure of discovery. UNSWCCL is particularly concerned that the interests of one of the major stakeholders in this process—the subscribers to and users of a service provider's facilities—have not been adequately addressed. In particular, our concerns relate to the need to:

- **restrict the breadth of discovery**
  - attempts by corporations to access subscriber details where it amounts to nothing more than an unwarranted attempt at 'fishing' should be curtailed;
  - when seeking discovery from a service provider, copyright holders should be required to have some identifying information about the potential infringer (e.g. a username);
  - copyright holders seeking discovery should be given access only to a narrowly specified class of documents;

- **protect the privacy of subscribers and users**
  - confidentiality agreements should be secured from all parties accessing personal data of subscribers during the course of litigation;
  - subscribers and other innocent parties should have the opportunity to identify privileged, confidential and private documents;
  - the overriding policy should be to protect the privacy of the subscribers and users of a service provider's facilities;

- **introduce strict procedures for making 'snapshots'**
  - there are currently no adequate procedures for the making of 'snapshot' copies of storage devices for the purposes of litigation;
  - there are currently no adequate warnings to subscribers that a 'snapshot' is to be made of the system.

[1] Phillips Fox, *Digital Review Agenda: Carriers and Carriage Service Providers Issue Paper* (July 2003) [5.3], [6.4.1]-[6.4.13]

[2] Philips Fox, above n 1, [5.4], [6.5.1]-[6.5.7]

Finally, UNSWCCL submits that the appropriate forum for adjudicating contentious discovery is the courts. If an alternative access regime is introduced (e.g. a procedure for voluntary disclosure of subscriber details), then the new regime must include strict and enforceable safeguards to guarantee confidentiality, to require the notification of the subscriber involved and the opportunity for the subscriber to identify privileged data, such as documents covered by legal professional privilege, and data protected by privacy legislation. Heavy penalties should attach to the infringement of these safeguards. Any procedure for voluntary disclosure must be truly voluntary and if it is challenged by the carrier and/or the subscriber, then disclosure should cease until the issue can be heard by a court.

2. The breadth of discovery

Currently, where a party wishes to seek a remedy for breach of copyright, but is unable to identify the wrongdoer, or does not have sufficient information to decide whether or not to institute proceedings, it may apply to the court to seek an order for discovery. Where such an order is directed against a service provider (e.g. a carrier, a carriage service provider or an Internet service provider), significant privacy concerns may arise.

One issue of concern is the breadth of the term 'document' and its application to mass storage devices. The Federal Court Rules and the *Evidence Act 1995* (Cwlth) define the term 'document' very broadly. It can include mass storage devices, such as hard disk drives, CD-ROMs, backup tapes, JAZ disks and ZIP disks. Hence, it is conceivable that an entire hard disk drive on a computer server may be considered a document that is discoverable and producible for inspection.

In the case of a service provider, it will hold personal information on a vast number of persons, many of whom would be unrelated to each other except for their subscription to the same service provider. Not only will a service provider hold the particulars of its subscribers and the logs of its subscribers' activities, but also it will store on its mass storage devices the personal work, files, correspondences and other information belonging to the subscribers or to persons other than the subscribers.

Clearly, the privacy implications of permitting access to the mass storage devices of service providers are significant. If this should occur, a party could obtain a great amount of information that is entirely irrelevant to the litigation at hand or in contemplation, but which may be private, confidential or privileged. Yet, given the broad definition of the term 'document', this is within the realm of possibility. Whether this will in fact occur will depend on the discretion of the court.

Discovery is a procedure that is provided for by the rules of court in each jurisdiction.[3] Nevertheless, the court retains discretion over the exercise of this procedure and it may refuse or limit discovery, as appropriate.[4] Some of the matters to which a court may have regard in the exercise of its discretion include the following:

- whether it would assist in the speedy and efficient resolution of the matters in dispute;
- whether it would cause unnecessary expense and delay;
- whether the extent of discovery sought would be oppressive;
- whether the documents, or class of documents, sought would be relevant to the issues in litigation; and
- whether it would be in the interests of justice to grant discovery.

[3] E.g., Federal Court Rules O 15A rr 3 and 6.
[4] *Burmah Oil Co. Ltd v. Bank of England* [1980] AC 1090 at 1141; *Ammerlaan v. Distillers Co. (Bio-Chemicals) Ltd* (1992) 58 SASR 164

Based on such considerations and the circumstances of the particular case, the court may restrict the extent of discovery sought. It would not be unusual for the court to require the party seeking discovery to agree to maintain confidentiality or to appoint an independent person to carry out inspection of the documents disclosed on discovery. Nevertheless, it is the view of UNSWCCL that this may not provide an adequate safeguard for protecting the privacy of subscribers.

As already mentioned, giving discovery to a service provider's mass storage devices may well result in the disclosure of information belonging to, or relating to, persons completely unrelated to the litigation concerned. Such innocent parties (some of whom may not even be subscribers of the service provider involved in the litigation) are unlikely to be aware that litigation is taking place and that it could result in the disclosure of information belonging to, or relating to, them. Hence, there is little possibility that such innocent parties will be in a position to represent their interests in court before discovery is given. For example, unbeknownst to the party giving discovery, an innocent party may have legitimate concerns that certain sensitive information should not be disclosed to the party seeking discovery. Further, such information may be completely unrelated to the issues in litigation.

As described above, such discovery is likely to occur in circumstances where a party does not have adequate information to commence proceedings. In such a situation, the issues in dispute are unlikely to be sufficiently defined and the identity of potential defendants may be unknown. This compounds the difficulty of narrowing down the information that is relevant for discovery. Inevitably, this allows a certain degree of 'fishing' to occur; and in the case of mass storage devices of service providers, it allows fishing through a mass of information belonging to, or relating to, innocent parties. Further, it has been held that the rules permitting discovery prior to the commencement of proceedings are beneficial in character and 'should be given the fullest scope its language will reasonably allow'.[5]

Therefore, while the court does carry out the exercise of balancing competing interests, in the case of mass storage devices belonging to service providers, an entire gamut of third party interests is unlikely to be represented before the court. Moreover, the rigour with which the court carries out its weighing exercise must inevitably be affected by the rigour with which a party resists discovery. It is unrealistic to expect that a party would necessarily resist discovery; or, if it does, its interests would not necessary coincide with those of other innocent third parties.

[5] *Paxus Services Ltd v. People Bank Pty Ltd* (1990) 20 IPR 79 per Burchett J at 85

In order that privacy implications are given due regard, UNSWCCL submits that the Digital Agenda should incorporate as one of its objectives the safegurading of the privacy of subcribers and users of facilities provided by service providers. This may be achieved by setting such an objective in the provisions of the *Copyright Act 1968*. In addition, to overcome the difficulties identified above, the *Copyright Act 1968* should be amended to provide for the following outcomes:

- attempts by corporations to access subscriber details where it amounts to nothing more than an unwarranted attempt at 'fishing' should be curtailed;
- when seeking discovery from a service provider, copyright holders should be required to have some identifying information about the potential infringer (e.g. a username);
- copyright holders seeking discovery should be given access only to a narrowly specified class of documents;
- confidentiality agreements should be secured from all parties accessing the personal data of subscribers during the course of litigation;
- subscribers and other innocent parties should have the opportunity to identify privileged, confidential and private documents;
- the overriding policy should be to protect the privacy of the subscribers and users of a service provider.

3. Alternatives to Existing Court Rules

3.1. current court rules are effective and sufficient

Subject to the recommended amendments set out above, UNSWCCL submits that the courts are the appropriate forum for adjudicating contentious discovery of both identification and documents.

As already noted, orders to disclose a person's identity, made pursuant to existing preliminary identification rules, are discretionary. In other words, the issuing of such an order is not a right, but is subject to the discretion of the court. Nothing beyond name, residential address, business address, occupation and gender should be provided.[6]

While a certain amount of 'fishing' is inevitable in identity discovery,[7] it is important to remember that judicial discretion is available to curtail the scope of discovery within reasonable limits.

The rules themselves also set a limit. For example, a party seeking preliminary discovery must have made *reasonable* inquiries to ascertain the identity of the persons against whom they intend to commence proceedings.[8]

Objections that current discovery procedures are time-consuming and expensive[9] fail to recognise that litigation *is* time-consuming and expensive. UNSWCCL acknowledges the overriding principle that litigation should be 'just, quick and cheap',[10] however we also submit that 'the ultimate aim of a court is the attainment of justice'[11] and that the privacy of individuals must not be compromised simply to satisfy the financial requirements of copyright holders.

- **UNSWCCL submits that the courts are the appropriate forum for adjudicating contentious discovery of both identification and documents.**
- **UNSWCCL does not recommend the introduction of a non-judicial subpoena for discovery of identification and documents, along the lines of United States rules.**

Furthermore, UNSWCCL is deeply concerned by the suggestion that judicial power be exercised by administrators.[12] This would expose Australians to a potential abuse of power against which our Constitution protects us. Such a process would undoubtedly be unconstitutional.[13]

[6] see for example: NSW Supreme Court Rules Pt 3 r1(3)
[7] *Sony Music Entertainment (Australia) Limited v University of Tasmania* [2003] FCA 532, [57] (Tamberlin J)
[8] Federal Court Rules O 15A r 3(1).
[9] see Philips Fox, above n 1, [6.4.6]
[10] NSW Supreme Court Rules Pt 1 r3
[11] *Qld v JL Holdings Pty Ltd* (1997) 141 ALR 353 (Dawson, Gaudron and McHugh JJ)
[12] Philips Fox, above n 1, [6.4.13]
[13] *R v Kirby; Ex parte Boilermakers' Society of Australia (Boilermakers case)* (1956) 94 CLR 254; see also, *Brandy v HREOC* (1995) 183 CLR 245.

3.2. The need for safeguards if alternatives are to be introduced

If the Attorney-General determines to recommend changes to the court rules, then UNSWCCL submits that there must be strict safeguards put in place to protect subscribers and users of carriers' and service providers' facilities.

Those safeguards should bear some resemblance to the orders in the *Universities cases*[14] and incorporate the standard rules for subpoenas.[15] Among other things:

- the requested data must be specified with *reasonable particularity*;
- the request must not be *oppressive*;
- the requested data must be *sufficiently relevant* to any intended action;
- only an independent consultant may examine computer logs, files and emails;
- that independent consultant must be party to a strict confidentiality agreement not to disclose what she or he sees;
- all parties affected must be given an opportunity to identify privileged, confidential and private data; and,
- heavy penalties should attach to a breach of this order.

Furthermore, if, despite concerns of constitutionality, the Attorney General determines to replicate the American non-judicial subpoena in Australia,[16] then cooperation should be *voluntary* for the same reasons that an *Anton Piller* order is not enforceable. That is, because such a subpoena is a civil and not a criminal procedure and does not amount to a search warrant—especially if it is not issued by a court. If any of the affected parties (carrier, service provider, subscriber or user) refuses to cooperate, then the applicant must go to the court for an *Anton Piller* order or a similar order.

[14] *Sony Music Entertainment (Australia) Limited v University of Tasmania* [2003] FCA 724 (18 July 2003)
[15] Federal Court Rules O 15A r8
[16] see Philips Fox, above n 1, [6.4.7]-[6.4.12]

4. Procedures for 'snapshots'

One important issue that appears to have been overlooked in the Review issue paper[17] is the procedure for preserving electronic documents and evidence. UNSWCCL is concerned that carriers and service providers are too willing to proceed with requests for extraordinarily broad 'snapshots' of whole computer systems without adequate warning to subscribers and users and without the supervision of a court.

In the *Universities case*,[18] Sony Music and Universal Music requested that a 'snapshot' of certain computers on the network belonging to the University of Tasmania be made to preserve evidence for future litigation against suspected infringers of their copyright. Copies were also made of hard disk drives in desktop computers used by nominated students.

UNSWCCL understands that a similar procedure was undertaken at the University of Sydney. There, a copy was made of a hard disk device belonging not to the university, but rather to a student of the university. The copies were made without consultation with the student concerned and without any warning. UNSWCCL is concerned about the privacy implications of such an unsupervised procedure.

These 'snapshots' are more intrusive and oppressive than standard system backups. They could, for example, involve:

- making a copy of files that are not usually backed up, such as full computer system and transactions logs and all hard disk storage devices on desktop computers, etc.; and,
- introducing system downtime during business hours while complete backups are made, as opposed to the quicker standard incremental daily backups of what has changed from day-to-day.

As well as the *content*, the *purpose* of the 'snapshot' is very different from the standard backup procedure. The 'snapshot' is not taken for business purposes, but rather for the purpose of preserving files for litigation. The *duration* of the retention of the 'snapshot' is also different from standard practice, which is to preserve records for a fixed period before erasing them. A 'snapshot', on the other hand, could be retained for an indefinite period.

[17] Philips Fox, above n 1

[18] *Sony Music Entertainment (Australia) Limited v University of Tasmania* [2003] FCA 532 (30 May 2003); *Sony Music Entertainment (Australia) Limited v University of Tasmania* [2003] FCA 724 (18 July 2003)

If a plaintiff can prove that there is a likelihood that a potential defendant might attempt to destroy evidence, it is standard procedure to have a *court* order the preservation of those documents. The standard order for preservation of evidence is called the *Anton Piller* order.[19] The 'appropriate undertakings or conditions…which…will ordinarily be required or imposed' in such an order include:[20]

- order must be executed during business hours;
- person to whom the order is directed should be advised of the right to obtain legal advice;
- an inventory of seized documents should be prepared and handed over to person to whom the order is directed;
- it may be appropriate for court to order that seized material be delivered to an independent custodian pending a court hearing of all parties; and,
- the independent custodian should be under an obligation not to disclose any of the information held.

Anton Piller orders are not enforceable, since they would otherwise amount to a search warrant.[21] A defendant may refuse access, but risks contempt of court proceedings.

There is no reason why such standards should not be applied to electronic data stored by carriers or service providers. Innocent users could have private, confidential or privileged data which they legitimately do not want preserved on a 'snapshot' and they should be permitted to chose to:

- remove the data before the 'snapshot' is taken;
- request that the data not be included in the 'snapshot'; or,
- refuse permission for the data to be included in the 'snapshot'.

UNSWCCL recommends that no 'snapshot' of a computer system should be taken for the purpose of preserving evidence without fair warning to all subscribers and users and a court order authorising, and defining the scope of, such an extraordinary procedure.

At the very least, subscribers and users should have the right to seek legal advice before the 'snapshot' is taken. The only way to do this is to provide fair warning to all subscribers and users who would potentially be effected.

These safeguards should help to relieve carriers and service providers of any liability resulting from the unauthorised copying of private, confidential or privileged data belonging to subscribers and users.

[19] *Anton Piller KG v Manufacturing Processes Ltd* [1976] Ch 55 (Court of Appeal, UK)
[20] Federal Court Practice Note 10 (*Anton Piller* orders)
[21] *Anton Piller KG v Manufacturing Processes Ltd* [1976] Ch 55 (Lord Denning MR)