



Privacy v Intellectual Property litigation: preliminary third party discovery on the Internet

Nic Suzor*

The enforcement of Intellectual Property rights poses one of the greatest current threats to the privacy of individuals online. Recent trends have shown that the balance between privacy and intellectual property enforcement has been shifted in favour of intellectual property owners. This article discusses the ways in which the scope of preliminary discovery and Anton Piller orders have been overly expanded in actions where large amounts of electronic information is available, especially against online intermediaries (service providers and content hosts). The victim in these cases is usually the end user whose privacy has been infringed without a right of reply and sometimes without notice.

This article proposes some ways in which the delicate balance can be restored, and considers some safeguards for user privacy. These safeguards include restructuring the threshold tests for discovery, limiting the scope of information disclosed, distinguishing identity discovery from information discovery, and distinguishing information preservation from preliminary discovery.

Contents

1. Tensions between privacy and intellectual property enforcement
 - 1.1 The need to protect privacy
 - 1.2 Obtaining private information from online intermediaries
 - National Privacy Principles
 - Breach of confidence and the tort of infringement of privacy
2. Eroding privacy through civil litigation
 - 2.1 Anton Piller orders
 - Lowering the thresholds: *Universal v Sharman*
 - 2.2 Equitable identity discovery
 - 2.3 Pre-action discovery under the rules of the court
 - Identity discovery
 - Information discovery from prospective respondent
 - Inspection and preservation of property
 - Blurring the distinctions: *Sony v University of Tasmania*
3. Restoring the balance — considering the privacy interests of affected parties
 - 3.1 Restructuring the threshold tests
 - Legitimising fishing

* BInfTech (QUT), LLB (QUT). The author would like to thank Professor Brian Fitzgerald, Sheryl Jackson, Dimitrios Eliades and Quentin Creagan for critique and feedback on this paper.

- 3.2 The distinction between identity and information discovery
- 3.3 Limiting the scope of identity discovery
- 3.4 Distinguishing information preservation from preliminary discovery
- 3.5 Restricting the scope of electronic information discovery
 - 'Documents' — separating relevant electronic files
 - Restricting access to 'transitory data'
 - Considering unrelated persons caught up
- 3.6 Defining the implied undertaking not to improperly use information
- 3.7 Rolling orders against unknown defendants
- 3.8 Safeguards in ex parte applications
 - Duty of candour
 - Amicus Curiae
- 3.9 Costs
- 3.10 Conclusion

1 Tensions between privacy and intellectual property enforcement

The enforcement of intellectual property rights poses one of the greatest current threats to the privacy of individuals online. In efforts to curb copyright infringement by Internet users, copyright owners have expended considerable effort on three main fronts: by building privacy invasive or usage limiting measures into technology via the development of Digital Rights Management techniques,¹ by lobbying for the criminalisation of circumvention of these technologies and harsher penalties for copyright enforcement,² and by litigation. Recent trends have shown that some copyright owners are becoming increasingly litigious, and increasingly prepared to bring suit against individuals.³ This article will address the ways in which intellectual property owners remove the privacy enjoyed by individuals on the Internet by harvesting information from online intermediaries — the service providers and content hosts.

This section will briefly outline the importance of privacy for individuals on the Internet, sketch the tensions between privacy and intellectual property

1 See, generally, G Greenleaf, 'IP, Phone Home: Privacy as Part of Copyright's Digital Commons, in Hong Kong and Australian law' in L Lessig, *Hochelaga Lectures 2002: The Innovation Commons*, Sweet & Maxwell, Asia, Hong Kong, 2003; J Cohen, 'Overcoming Property: Does Copyright Trump Privacy' [2003] 1 *Uni of Illinois Jnl of Law, Technology & Policy* 101; L Bygrave, 'The Technologisation of Copyright: Implications for Privacy and Related Interests' (2002) 24 *European Intellectual Property Rev* 51; J Cohen, 'A Right To Read Anonymously: A Closer Look At "Copyright Management" In Cyberspace' (1996) 28 *Conn L Rev* 981.

2 Digital Millennium Copyright Act 17 USC 17 § 1201 (2000); Copyright Act (Digital Agenda) Act 2000 (Cth); Protecting Intellectual Rights Against Theft and Expropriation (PIRATE) Bill 108TH Congress 2D Session (2004); Inducing Infringement of Copyrights (INDUCE) Bill 108TH Congress 2D Session (2004).

3 See, for example, *Universal Music Australia Pty Ltd v Miyamoto* [2003] FCA 812 (unreported, Lindgren J, 18 July 2003, BC200304255) (where 'John Doe' orders were initially taken out); *Universal Music Australia Pty Ltd v Hendy Petroleum Pty Ltd* (2003) 59 IPR 204; *Kabushiki Kaisha Sony Computer Entertainment v Stevens* (2003) 200 ALR 96; 57 IPR 161.

enforcement, and discuss why it is difficult for intellectual property holders to obtain information from intermediaries without recourse to litigation. Part 2 will outline two ways in which private information can be sought by litigants from intermediaries, namely Anton Piller orders and preliminary discovery, and highlight some recent examples of excessive preliminary discovery being granted at the expense of privacy. Finally, Part 3 will discuss some of the ways in which the law can develop to more fully protect the privacy of individuals on the Internet, by restoring the delicate balance between intellectual property rights and privacy rights.

1.1 The need to protect privacy

Privacy is a notoriously difficult concept to define.⁴ One of the most influential definitions has been that of Samuel Warren and Louis Brandeis who, in 1890, argued that the right to privacy in the United States formed part of a broad right 'to be let alone'.⁵ Alan Westin, in 1967, argued that 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.⁶ Another broadly supported definition is that of Ruth Gavinson, who argued that the right of privacy was dependant on 'limited access', and consisted of 'three independent and irreducible elements: secrecy, anonymity, and solitude'.⁷ Lee Bygrave argues that this last conception of privacy 'comes closest to capturing the core of the concept at the same time as it does relatively large justice to the concept's multidimensionality'.⁸

Evidently, none of the various definitions of privacy are complete, and all overlap in some way. An exact definition of privacy is not as important as a general recognition of its importance. The Australian Privacy Charter states that:

A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organisations to intrude on that autonomy.⁹

Privacy rights are assuming more significance with the increase of the capabilities for their erosion. Justice Michael Kirby, writing extrajudicially, has succinctly noted the effects of technological advances on the way privacy was traditionally protected:

The speed, power, accessibility and storage capacity for personal information identifying an individual are now greatly increased. Some of the chief protections for privacy in the past arose from the sheer costs for retrieving personal information; the impermanency of the forms in which that information was stored; and the inconvenience experienced in procuring access (assuming that its existence was known). Other protections for privacy arose from the incompatibility of collections

4 See, for example, D J Solove, 'Conceptualizing Privacy' (2002) 90 *Calif L Rev* 1087 at 1088.

5 S D Warren and L D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard L Rev* 193 at 195.

6 A F Westin, *Privacy and Freedom*, Athenaeum, New York, 1967, p 7.

7 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Jnl* 421 at 433.

8 L Bygrave, 'The Place Of Privacy In Data Protection Law' [2001] *UNSWLJ* 6 at n 11.

9 Australian Privacy Charter Council, 'The Australian Privacy Charter' [1995] *PLPR* 31 at 31.

with available indexes and the effective undiscoverability of most personal data. These practical safeguards for privacy largely disappear in the digital age.¹⁰

Jack Balkin has recognised that privacy goes to the heart of 'individualism and individual autonomy'.¹¹ Balkin argues that redefining privacy and determining proper limits on enforcing privacy rights in the face of rapidly changing technology becomes a discourse about the new forms of power and control, and about technological change and 'who has control over its shape and direction'.¹²

This concept of control over technological change has never been more important. In this particular struggle, the parallel technological advancement to the greater ability to remove privacy is the greater capacity for copyright infringement to take place. The growing capabilities of compression techniques to reduce the size of digital media while increasing its quality, the increased bandwidth available to home users, and the ease of use of modern filesharing technologies all contribute to a much greater scope of copyright infringement amongst individuals than was previously possible.

Part of the struggle between privacy and copyright enforcement is over the way that technology should develop, to favour the rights of individuals or the rights of intellectual property owners.¹³ The other part of the struggle is the struggle over the fruits of technology. This is a struggle about how technology can be used, and about when certain actions that technology makes possible must be restricted. Different views of the possibilities afforded by technological changes are championed by each side, and a delicate balance must be continuously struck as rights and perceptions of rights change.

This struggle is importantly visible in recent litigation between intellectual property owners and online intermediaries. Specifically, the struggle relates to what access third parties should have to the wide range of potentially private information that is made harvestable by technology. As will be demonstrated, the recent trend has been to favour protection of intellectual property over the privacy rights of individuals.

1.2 Obtaining private information from online intermediaries

Traditionally, gathering information about individuals from intermediaries has been difficult, particularly because the infrastructure of the Internet was designed to avoid concentrating power and control in central entities, leaving only the parties to a communication responsible for that communication.¹⁴ Organisations frustrated by the unavailability of this information have identified intermediary nodes on the Internet as the next most appropriate targets for both regulation and information gathering: the Internet Service

10 See M D Kirby, 'Privacy in Cyberspace' (1998) 21(2) *UNSWLJ* 323 at 325.

11 J M Balkin, 'What is a Postmodern Constitutionalism?' (1992) 90 *Mich L Rev* 1966 at 1988.

12 *Ibid.*

13 See above n 1.

14 See, generally, L Lessig and M Lemley, 'The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era' (April 2001) 48 *UCLA L Rev* 925.

Providers (ISPs), who provide Internet access to end users, and content hosts, who provide the Internet servers, services and content that enables end users to communicate with each other.

A content host provides users with a method of locating and accessing information, either supplied by that host, or available through another host or user. Content hosts include web servers, file servers, web forums, Internet Relay Chat (IRC) servers, and Peer-to-Peer filesharing servers, which all provide the infrastructure for users to locate and communicate with each other. Sometimes the communications between users occurs wholly through the content provider, and sometimes the users communicate independently once they have located each other through the content provider. Importantly, the content provider often does not exercise any control over, nor have any knowledge about, the actions of users, making it very difficult for it to attract any liability when those actions infringe another organisation's rights.¹⁵ The servers do, however, often record information regarding access to resources by users. Where the provider does not log this information, it none the less passes through the provider's networks, and is technically able to be captured if required.

Often, the information gathered from content hosts can not completely identify users; transactions between users and content hosts are usually carried out anonymously or pseudonymously. The users may be only identified by their IP address, which is an address specific to each computer that is connected to the Internet, but often routinely changed and recycled between end users. To identify an individual from an IP address, an organisation will often have to obtain further information from an Internet Service Provider, which can identify an account holder given the address and time of access, assuming appropriate logs were kept.¹⁶

It is difficult to gather this type of information from intermediaries without resort to the legal system. Section 105 of the Telecommunications (Interception) Act 1979 (Cth) provides that it is an offence to intercept communications. Section 276 of the Telecommunications Act 1997 (Cth) provides that it is an offence to disclose or use any information or document that relates to 'the contents or substance of a communication that has been carried by a carrier or carriage service provider', 'the contents or substance of a communication that is being carried', 'carriage services supplied, or intended to be supplied, to another person', or 'the affairs or personal particulars . . . of another person'.¹⁷ These provisions mean that the content of communications can not legally be intercepted, disclosed or used by Internet intermediaries. The *existence* of those communications, on the other hand, and

¹⁵ See *CoStar Group, Inc v LoopNet, Inc*, No 03-1911 (4th Cir, 21 June 2004).

¹⁶ It is never possible to identify an *individual* from an IP address — the best that a service provider can do is identify an account holder or a telephone number from which the service was accessed.

¹⁷ Section 276(1)(a)(i)–(iv). See also *Blumofe v Pharmatrak, Inc (In re Pharmatrak Privacy Litig)* 329 F 3d 9 (2003), where the US First Circuit Court of Appeal held that a service which was employed to collect traffic and usage statistics from certain pharmaceutical websites, but in fact also collected some personal and identifying data, 'intercepted' communications for the purposes of the Electronic Communications Privacy Act of 1986 (ECPA), 18 USC §§ 2511, 2520 (2000).

details relating to the provider's activities, for example the routing of communications to a specific network or location, the time, date, size and frequency of the communication could conceivably be recorded and possibly disclosed.

There is an exception to these rules where the disclosure or use is 'required or authorised by law'.¹⁸ In *Re Telstra*,¹⁹ Burchett J considered that it was prudent for Telstra to seek an order for identity discovery before it searched its own records to identify a customer. Another exception to the rule applies when 'the disclosure or use is made in the performance of the person's duties as . . . an employee'.²⁰ Burchett J left open the question as to whether the information sought could have been disclosed and used in this way. Certainly it is not unthinkable (though perhaps somewhat undesirable) that where a provider's business activities included disclosing such information, these rules would not apply.

Where criminal liability under these two Acts does not attach to a disclosure of information, individuals affected may have to rely, after the fact, on formal complaints under privacy laws or civil actions against the provider and the person to whom the information was disclosed.

National Privacy Principles

Following the Privacy Amendment (Private Sector) Act 2000 (Cth), the Privacy Act 1988 (Cth) requires private organisations with an annual turnover of greater than \$3 million to act in accordance with an approved code of conduct or with the National Privacy Principles (NPPs) when dealing with personal information.²¹

The requirements of the Privacy Act can be sidestepped in three important ways. Firstly, since compliance with an approved code of conduct guarantees that the Privacy Act will be complied with, codes of conduct have the potential to override the National Privacy Principles, providing for situations, for example, where ISPs will voluntarily log as much information as they can without breaching the Telecommunications (Interception) Act 1979, and have no defined policy on the disclosure of such information to persons other than enforcement agencies.²² The second way is where the user consents to the disclosure. This 'consent' can be deemed to have been given by inserting clauses in the Terms of Service (ToS) or End User Licence Agreements (EULAs), which often go unread by users on the Internet. Thirdly, information on a user's activities online could arguably not be information protected by the Act, because although the account holder and even the location of the user can be ascertained, it is not possible to identify the actual person using the account at that time. This means that the information is arguably not about an

18 Section 280 (1)(b).

19 *Re Telstra Corp Ltd* [2000] FCA 682 (unreported, Burchett J, 17 May 2000, BC200002815).

20 Section 279(1).

21 Privacy Act 1988 s 16A.

22 See, for example, Internet Industry Association's draft 'Cybercrime Code Of Practice' (public consultation draft 2.0, July 2003) <[http://www.ii.net.au/cybercrime_code_v2\(chn\).doc](http://www.ii.net.au/cybercrime_code_v2(chn).doc)> (accessed 8 July 2004).

‘individual’, as required by the Privacy Act,²³ but information about an account holder.

Where the privacy principles do apply, NPP 1.1 states that an ‘organisation must not collect personal information unless the information is necessary for one or more of its functions or activities’.²⁴ ISPs and content hosts can legitimately collect and store detailed information on users’ online activities, if doing so would be necessary to, for example, streamline content delivery, structure marketing procedures, or manage resource allocations. In a lot of cases, these activities will not require personal information — there is often no requirement that the information be stored in a form which allows the user to be identified, as opposed to aggregate statistics. However, it must be assumed that there will be some legitimate activities that will require the information to be traceable at least to a user account or IP address.

NPP 10.1 prohibits the collection of *sensitive information*. ‘Sensitive information’ includes information about an individual’s racial or ethnic origin, political opinions, membership of political, professional or trade associations or unions, religious or philosophical beliefs, sexual preferences or practices, and criminal record.²⁵ Information that relates to an individual’s activities on the Internet could, depending on how specific it is, be considered to be ‘sensitive information’. The restriction on the collection of this information does not apply where the individual has consented, the collection is required by law, or the collection is ‘necessary for the establishment, exercise or defence of a legal or equitable claim’.²⁶ It would usually be the case that such a ‘legal or equitable claim’ would relate to a claim by or against the provider, but this is not necessarily the case. A wide interpretation of this exception would allow sensitive information to be collected if the provider decided, on some request from an IP owner, to aid in the investigation of a claim on behalf of the IP owner.

NPP 2 establishes the general rule that personal information must only be used or disclosed for the primary purpose for which it was collected. In general, for intermediaries, this would not include disclosing usage activities to copyright owners. However, NPP 2.1(f) allows an organisation to disclose personal or sensitive information when it ‘has reason to suspect that unlawful activity has been, is being or may be engaged in’, as long as the disclosure is a ‘necessary part of its investigation of the matter’, or is disclosure to ‘relevant persons or authorities’. It is arguable that ‘unlawful activity’ will extend to infringements of copyright, and that a ‘relevant person’ would include the copyright owner. Accordingly, where a copyright owner alleges a breach of copyright, an intermediary may be justified in disclosing any information it has relating to the claim.

At any rate, a term in the Terms of Service of providers can always exclude the operation of the NPPs by providing ‘consent’ for the disclosure of personal information. Given the small number of ISPs in Australia,²⁷ and their

23 Privacy Act 1988 (Cth) s 6.

24 Ibid, Sch 3, 1.

25 Ibid, s 6.

26 Ibid, Sch 3, 10.1.

27 The Australian Bureau of Statistics reports that six ‘very large’ ISPs (100,000+ subscribers)

associated high relative bargaining strengths as compared to that of consumers, the private sector amendments to the Privacy Act do not go far enough to protect Australian Internet users, and affected users may have to turn to civil remedies to protect their rights.

Breach of confidence and the tort of infringement of privacy

There is no generally accepted common law action for invasion of privacy in Australia. In *Grosse v Purvis*, Skoien SJ, in the Queensland District Court, recognised the existence of a tort of invasion of privacy, without setting down the exact limits of the cause of action or any defences.²⁸ It is important to note that this decision is not binding on any interstate or federal jurisdiction, and concerned what was essentially a stalking case. As such, it is not clear whether the decision will be followed or expanded in the circumstances with which we are concerned. The House of Lords recently rejected this approach to a tort of privacy.²⁹ On the other hand, the New Zealand Court of Appeal, in a 3-2 majority, has affirmed the existence of the tort in quite broad terms that will restrain publication of facts in which there is a reasonable expectation of privacy.³⁰ In Australia, the weight of passing off and trade practices authorities before *Grosse v Purvis* generally require a substantial reputation in the jurisdiction before acting to enforce what are essentially privacy rights,³¹ and Heerey J in the Federal Court has recently held that the weight of authority so far is against an independent tort of privacy.³²

Whether or not an independent Australian tort of invasion of privacy is recognised may not have a great impact, in that it may afford much the same protection as the rapidly developing equitable action for breach of confidence.³³ Over the last 15 years, the action for breach of confidence has developed in a broad trend from protecting classically confidential information towards protecting the privacy of individuals.³⁴ The action will restrict a person from using or disclosing information which has been

provide access to 68% of Australian Internet subscribers (Australian Bureau of Statistics, *8153.0 Internet Activity, Australia*, September 2003).

28 (2003) Aust Torts Reps 81-706.

29 *Wainwright v Home Office* [2003] 4 All ER 969.

30 *Hosking v Runting* (2004) 7 HRNZ 301. Gault P and Blanchard J, at [117], expressed the elements of the action as: '1. The existence of facts in respect of which there is a reasonable expectation of privacy; and 2. Publicity given to those private facts that would be considered highly offensive to an objective reasonable person'. Tipping J went further at [259], holding that 'It is actionable as a tort to publish information or material in respect of which the plaintiff has a reasonable expectation of privacy, unless that information or material constitutes a matter of legitimate public concern justifying publication in the public interest.'

31 See *10th Cantanae Pty Ltd v Shoshana Pty Ltd (Sue Smith Case)* (1987) 79 ALR 299; 10 IPR 289; *Honey v Australian Airlines Ltd (Gary Honey case)* (1990) 18 IPR 185; *Talmax Pty Ltd v Telstra Corporation Ltd (Kieran Perkins case)* (1996) ATPR 41-484.

32 *Kalaba v Commonwealth of Australia* [2004] FCA 763 (unreported, Heerey J, 8 June 2004, BC200403700) at [6].

33 See *Hosking v Runting* (2004) 7 HRNZ 301 at [247] per Tipping J: 'The result in substantive terms of recognising a separate tort is not significantly different from the extended form of the breach of confidence cause of action as it is being developed in the United Kingdom. What is at stake is really a matter of legal method rather than substantive outcome.'

34 See *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 at 281; [1988] 3 All ER 545 at 658 per Lord Goff; *A v B plc* [2003] QB 195 at 202; [2002] 2 All ER 545.

imparted in a way which gives rise to an obligation of confidence.³⁵ The expansion of the action has reached an extent where it may restrain online intermediaries from disclosing information on users' activities to third parties.

There is no particular type of information that will be protected. It is sufficient that the information is not trivial,³⁶ and is of a confidential nature.³⁷ This means that the information cannot be public knowledge,³⁸ but it need only be relatively secret.³⁹ The focus of the doctrine is on respecting circumstances of confidence, not on protecting the information itself.⁴⁰

The other element to the action is the requirement that the information be given in a situation which imports an obligation of confidence. It is now generally settled that this requirement no longer needs a pre-existing confidential relationship.⁴¹ In *ABC v Lenah*, Gleeson CJ remarked, obiter, that the publication of a videotape of private information, taken from a hidden camera, could be restrained; the duty will arise where 'disclosure . . . would be highly offensive to a reasonable person of ordinary sensibilities'.⁴² In *Douglas v Hello!*,⁴³ Lindsay J held that the unconscionable surreptitious photographing of confidential or private information gave rise to an action for breach of confidence. Recently, in *Campbell v MGN*, the House of Lords considered that the duty will arise where a person 'knows or ought to know that there is a reasonable expectation that the information in question will be kept confidential'.⁴⁴ The removal of the need to show a relationship of confidence means that the doctrine has the potential to protect much of the information that intermediaries on the Internet have access to as it passes through their systems. However, it is important to note that a person communicating on the Internet may be consenting to 'such risks of being overheard as are inherent in the system'.⁴⁵

It is suggested that in cases where intermediaries on the Internet collect and disclose users' detailed transaction data (excluding, of course, disclosure

35 *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* [1963] 3 All ER 413 at 414 per Lord Greene MR; *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41 at 48 per Megarry J.

36 *Stephens v Avery* [1988] Ch 449; [1988] 2 All ER 477.

37 *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41.

38 *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* [1963] 3 All ER 413.

39 *Ansell Rubber Co Pty Ltd v Allied Rubber Industries Pty Ltd* [1967] VR 37.

40 D Lindsay, 'Playing possum? Privacy, freedom of speech and the media following *ABC v Lenah Game Meats Pty Ltd*. Part II: The future of Australian privacy and free speech law, and implications for the media' (2002) 7(2) *Media & Arts L Rev* 161 at 167, citing F Gurry, 'Breach of Confidence' in P Finn (Ed), *Essays in Equity*, Law Book Co, North Ryde, 1985, p 116.

41 *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 at 281; [1988] 3 All ER 545 at 658 per Lord Goff; *A v B plc* [2003] QB 195 at 207; [2002] 2 All ER 545.

42 *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199; 185 ALR 1 at [42]. Note that the information in this case was not considered *private*, and hence did not attract the protection of breach of confidence.

43 [2003] 3 All ER 996, (approved judgment).

44 [2004] 2 All ER 995 at [134] per Baroness Hale; see also [85] per Lord Hope of Craighead ('a duty of confidence will arise whenever the party subject to the duty is in a situation where he knows or ought to know that the other person can reasonably expect his privacy to be protected'); [21] per Lord Nicholls (dissenting) ('reasonable expectation of privacy').

45 *Malone v Metropolitan Commissioner* [1979] Ch 344 at 376; [1979] 2 All ER 620. In this case Megarry VC was referring to the telephone system, but the principle seems equally applicable to the Internet.

required by law), an action for breach of confidence may be appropriate. Further development of the doctrine by the courts will be necessary, as the limits of what types of data will be deemed 'confidential' are not clear,⁴⁶ but these developments would not be a large step from the current law. The disadvantage with this proposition is that remedies only become available after the information has been disclosed (or disclosure is threatened), and the burden is placed upon the affected individual to prove their case. It would seem much more prudent to adopt a position where civil remedies are a last resort, and a person who seeks to remove an individual's privacy must adequately show that it is justified in doing so, before the fact.

2 Eroding privacy through civil litigation

Because of the difficulty and potential problems associated with obtaining information from intermediaries without the sanction of the legal system, intellectual property holders are increasingly turning to civil litigation in order to force disclosure. In this section, we are concerned with the most intrusive forms of compulsory disclosure, specifically Anton Piller orders and preliminary third party discovery.

2.1 Anton Piller orders

Anton Piller orders have been described as 'civil search warrants'⁴⁷ and the 'nuclear weapons of the law'.⁴⁸ They are designed to allow applicants to seize documents or other things from respondents, to prevent the injustice that would arise if they were lost or destroyed. The order acts in personam, directing the respondent that he or she should allow the applicant to enter his or her premises, in order to find and remove certain documents or things. It does not authorise the applicant to enter the premises, but does provide that if the respondent does not allow the applicant to enter, he or she may be guilty of contempt of court.

The order is named after the 1976 English Court of Appeal case *Anton Piller KG v Manufacturing Processes Ltd*,⁴⁹ which delimited its scope and application. In that case, Denning LJ held that the order should only be made where:

it is essential that the plaintiff should have inspection so that justice can be done between the parties; and when, if the defendant were forewarned, there is a grave danger that vital evidence will be destroyed, that papers will be burnt or lost or hidden, or taken beyond the jurisdiction, and so that the ends of justice be defeated; and when the inspection would do no real harm to the defendant or his case.⁵⁰

In the same case, Omrod LJ set out the essential pre-conditions for the order:

⁴⁶ For example, merely encrypting data does not impart an obligation of confidence: *Mars UK Ltd v Teknowledge Ltd* (1999) 46 IPR 248 at 256.

⁴⁷ P Godin, 'Anton Piller Orders in an Age of Scepticism: Charter Application and Other Safeguards for Judicially-Ordered Searches' (1996) 54 *UT Fac L Rev* 107, citing *Indian Manufacturing Ltd v Lo* (unreported, 28 September 1995) (FCTD) per Reed J.

⁴⁸ *Bank Mellat v Nikpour* [1985] FSR 87 at 92 (CA) per Donaldson LJ.

⁴⁹ [1976] Ch 55; [1976] 1 All ER 779.

⁵⁰ *Ibid*, at Ch 61B; All ER 783 per Denning LJ.

First, there must be an extremely strong prima facie case. Secondly, the damage, potential or actual, must be very serious for the plaintiff. Thirdly, there must be clear evidence that the defendants have in their possession incriminating documents or things, and that there is a real possibility that they may destroy such material before any application inter partes can be made.⁵¹

In Australia, jurisdiction to make the order is derived from the inherent jurisdiction of superior courts of record,⁵² but also conferred by statute in the Federal Court,⁵³ and regulated by the rules of the court or practice notes in some jurisdictions.⁵⁴ The order is designed to safeguard evidence in proceedings before notice is given to the defendants. As such, it is made ex parte, and sometimes in camera,⁵⁵ and will generally not be available after proceedings have been initiated.⁵⁶

It is generally recognised that the orders should not allow the plaintiff to trawl through extensive records seeking to identify possible infringements or possible defendants — the information should be used to strengthen or facilitate contemplated actions, not to find new causes of action. In *Hytrac Conveyors v Conveyors International*, Lawton J noted that:

Those who make charges must state right at the beginning what they are and what facts they are based on. They must not use Anton Piller orders as a means of finding out what sort of charges they can make.⁵⁷

An applicant must show a strong prima facie case against the respondent before the order will be granted. Accordingly, the order should not be granted against intermediaries or other third parties — third party discovery provides a much less intrusive and more controlled method of obtaining information from third parties. It has been recognised, however, that the information seized is often used to identify and take action against previously unknown parties.⁵⁸

51 Ibid, at Ch 62A; All ER 784 per Omrod LJ, cited with approval by Lee J in *Television Broadcasts v Nguyen* (1988) 21 FCR 34 at 38; 15 IPR 97 at 102.

52 *Simsek v Minister For Immigration and Ethnic Affairs* (1982) 40 ALR 61 at 65.

53 Section 23 of the Federal Court of Australia Act 1976 (Cth); see also *Television Broadcasts v Nguyen* (1988) 21 FCR 34 at 38; 15 IPR 97 at 102.

54 Federal Court of Australia, Practice Note No 10; Australian Capital Territory Supreme Court, Practice Direction No 4 (1994); Uniform Civil Procedure Rules (Qld) r 261; South Australia Supreme Court, Practice Direction 48.

55 See *Golf Lynx v Golf Scene Pty Ltd* (1984) 75 FLR 303 at 312 per Legoe J (SA SC).

56 *Microsoft Corp v Goodview Electronics Pty Ltd* (1999) 46 IPR 159.

57 [1982] 3 All ER 415 at 418 per Lawton J.

58 See *Iomega Corporation v Myrica (UK)* (1999) SLT 796; 1998 SCLR 475 (Scottish Court Of Session: Inner House (First Div)):

I suspect that in practice documents must quite frequently have been used as the basis of proceedings in other actions. For example, a pursuer may recover documents and discover from them that he has sued the wrong person and that the appropriate defender is, say, a different company. I should be surprised if it were argued that he could not be permitted to use the documents in fresh proceedings against the other company without first returning them to the haver and then solemnly seeking a fresh commission and diligence in the new proceedings. Similarly, a pursuer may discover from the documents which he has recovered that he should also have sued someone else as a defender. He may, of course, amend to add that person as an additional defender in the same proceedings, but he could equally competently sue him in a separate action. If he could use the documents in the proceedings to which the new person had been added as a

Lowering the thresholds: *Universal v Sharman*

In February 2004, a number of record labels sought and obtained an Anton Piller order against Sharman Networks, the operators of the Kazaa filesharing network. After the execution of the order, the respondents unsuccessfully applied to have the orders set aside.⁵⁹ The decision to grant the Anton Piller order is alarming for two reasons: the threshold tests appear to have been lowered substantially, and the scope of the order, and the information disclosed, was extremely broad. Unfortunately, the application to set aside the order did not address these concerns, but focused on the fact that when making the ex parte application, Universal had not disclosed all significant details of the substantially similar litigation on foot in the United States, *MGM v Grokster*.⁶⁰

Kazaa is a peer-to-peer filesharing network which provides a means for users to communicate with each other and send and receive digital files amongst themselves. The system works differently to older peer-to-peer filesharing networks, like Napster and Aimster, whose operators were held to be indirectly liable for copyright infringement,⁶¹ in that the operators arguably have no knowledge and exercise no control over the activities of users.⁶² The Anton Piller order sought in this case was important to the applicants, because the information seized would allow them to investigate whether there was any way indirect copyright liability could attach to the operators of the network, or to a special class of users called 'supernodes'.⁶³ Without this information, the recording industry could only continue to bring actions against individuals, a move which is considerably unpopular.⁶⁴

defender by amendment, I can see no reason in principle why he should not equally be permitted to use them in separate parallel proceedings.

Cf *Crest Homes plc v Marks* [1987] AC 829 at 853; [1987] 2 All ER 1074 at 1078 per Lord Oliver: 'to use a document obtained on discovery in one action as the foundation for a claim in a *different and wholly unrelated* proceeding would be a clear breach of the implied undertaking [not to use the material improperly]' (emphasis added).

⁵⁹ *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2004) 205 ALR 319; 59 IPR 299. The respondents have applied for leave to appeal from the interlocutory judgment to the Full Court of the Federal Court. See *Brilliant Digital Entertainment Pty Ltd v Universal Music Australia Pty Ltd* [2004] FCA 448 (unreported, Tamberlin J, 16 April 2004, BC200401893). The appeal appears at this stage to be based mainly on the question of Sharman's cooperation with the plaintiffs and the lack of disclosure given by Universal.

⁶⁰ *Metro-Goldwyn-Mayer Studios, Inc v Grokster, Ltd* 259 F Supp 2d 1029 (CD Cal 2003), appeal pending, No 03-55901 (9th Cir argued 3 February 2004).

⁶¹ *A&M Records, Inc v Napster, Inc* 114 F Supp 2d 896 (ND Cal 2000); *Re Aimster Copyright Litigation* (2003) 334 F 3d 643. *Aimster* was an interlocutory injunction to shut down the Aimster network before trial, resulting in the collapse of the organisation.

⁶² *Metro-Goldwyn-Mayer Studios, Inc v Grokster, Ltd*, 259 F Supp 2d 1029 (CD Cal 2003), appeal pending, No 03-55901 (9th Cir argued 3 February 2004).

⁶³ A supernode is an ordinary user of the network with a more powerful computer or Internet connection that has been designated as a point of contact between users and indexing files and processing search requests. These supernodes connect to other supernodes, forming a distributed web of connections. In most cases, a user will not be aware that they are acting as a supernode, as the process is generally automated.

⁶⁴ See FindLaw, 'FindLaw Survey Reveals RIAA Lawsuits Unpopular with Americans', 29 June 2004, <<http://company.findlaw.com/pr/2004/062904.musicpiracy.html>> (accessed 11 July 2004): 56% of adult Americans oppose the Recording Industry Association of America's numerous lawsuits against individual users of filesharing applications.

Threshold tests

As stated above, the three limbs of the widely accepted test expressed by Omrod LJ in *Anton Piller* require that there is a strong prima facie case, very serious actual or potential damage, and a real possibility that the defendant will destroy incriminating documents or things that they have in their possession.

Indirect liability for copyright infringement in Australia is primarily drawn from s 36 of the Copyright Act 1968 (Cth), which prohibits ‘authorisation’ of copyright infringement. In *University of New South Wales v Moorhouse*,⁶⁵ a case which dealt with the provision of photocopiers in university libraries, Gibbs J enunciated the test for authorisation:

a person who has under his control the means by which an infringement of copyright may be committed — such as a photocopying machine — and who makes it available to other persons, knowing, or having reason to suspect, that it is likely to be used for the purpose of committing an infringement, and omitting to take reasonable steps to limit its use to legitimate purposes, would authorise any infringement that resulted from its use.⁶⁶

In the US case of *Sony v Universal* (the ‘Betamax’ case),⁶⁷ it was held that the manufacturer of VCRs could not be held responsible for any infringing use of those VCRs because they had relinquished control of the means of infringement. In *Grokster*, the US District Court held that the operators of substantially similar peer-to-peer networks did not attract secondary liability for copyright infringement because they did not have actual knowledge of infringements at a time at which they could exercise some control over the activities of their users.⁶⁸ Nicholas Blackmore has suggested that it would be open for an Australian court to follow US authority and qualify the *Moorhouse* test with a requirement that control be held at the time of the infringement.⁶⁹

In the application for the Anton Piller order in *Sharman*, the applicants stated that:

there remain significant features of the Kazaa system about which the applicants have not been able to obtain detailed knowledge. These include the nature and extent of communications passing between various elements of the Kazaa system, including encrypted communications, the content of such communications, and the existence and operation of mechanisms used by the operators, programmers and administrators of the Kazaa system to control or monitor aspects of the system.⁷⁰

These ‘features’ of the Kazaa system are decisive factors in whether or not Sharman can be indirectly liable for copyright infringement. Levels of control, actual or implied knowledge and reasonable steps to prevent infringement are all directly relevant under the test in *Moorhouse*. The same factors are even

⁶⁵ *University of New South Wales v Moorhouse and Angus & Robertson (Publishers) Pty Ltd* (1975) 133 CLR 1; 6 ALR 193.

⁶⁶ *Ibid*, at CLR 13; ALR 200.

⁶⁷ 659 F 2d 963 (9th Cir 1981), cert granted, 102 S Ct 2926 (1982) (No 81-1687).

⁶⁸ *Metro-Goldwyn-Mayer Studios, Inc v Grokster, Ltd* 259 F Supp 2d 1029 (CD Cal 2003), appeal pending, No 03-55901 (9th Cir argued 3 February 2004).

⁶⁹ N Blackmore, ‘Peer-To-Peer Filesharing Networks: The Legal and Technological Challenges for Copyright Owners’ (2004) 55 *Computers & Law* 7.

⁷⁰ *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2004) 205 ALR 319; 59 IPR 299 at [10].

more relevant in light of (non binding) US authority after *Grokster*. Sharman's indirect liability for copyright infringement is debatable, and can not be said to approach the required standard of an 'extremely strong prima facie case'.⁷¹ The other two grounds relied upon by the applicants were direct infringement of the right to communicate sound recordings to the public,⁷² and joint liability in the statutory tort of copyright infringement. Similarly, neither of these grounds apparently shows a strong prima facie case, because any infringement of copyright on the Kazaa network would generally be occurring between users, without any further involvement of Sharman. Although the applicants contended that they had a strong prima facie case, the facts and applicable law do not appear that simple.

The second limb of the test to grant an Anton Piller order requires that there must be very serious actual or potential damage to the plaintiff. It is not necessary for our purposes to examine the degree of damage caused by illegitimate filesharing. It is sufficient to note that there is recent empirical evidence that suggests that the damage, in lost record sales, associated with filesharing is not as significant as publishers have feared.⁷³

The final limb of the test expressed by *Omrod LJ* requires that there is a 'real possibility' that defendants would destroy the information in their possession if given notice of the action. Leaving aside the question of whether the same type of information was already provided by the same defendants to the same plaintiffs in the action in the United States, *Wilcox J* considered that the nature of the operation of the system necessitated that steps be taken to preserve the transient information that flows through the system:

Evidence about dynamic operation is available on relevant computers, from moment to moment, as the transactions occur. If that evidence is to be available at the trial, there must be 'snapshots', perhaps many snapshots, showing the changing data in the system from moment to moment. The scheme of the Anton Piller orders was to allow those snapshots to be taken, and thereby to preserve that changing data. Analysis of the data will no doubt add to the experts' understanding of the operation of the Kazaa system, but that does not mean that the exercise permitted by the Anton Piller orders was an investigation. It was an exercise designed to preserve evidence.⁷⁴

By definition, every case that concerns online transactions will involve 'transitory' data to some extent. The expansion of Anton Piller orders shown in this case means that an applicant can obtain a highly disruptive order without satisfactorily demonstrating a strong prima facie case and without showing a risk that the respondent will destroy the information if he or she is

⁷¹ *Anton Piller KG v Manufacturing Processes Ltd* [1976] Ch 55 at 62A; [1976] 1 All ER 779 at 784 per *Omrod LJ*.

⁷² Copyright Act 1968 (Cth) s 85(1)(a), (c).

⁷³ See F Oberholzer and K Strumpf, 'The Effect of File Sharing on Record Sales: An Empirical Analysis', <[http://www.unc.edu/\[cigar/papers/FileSharing_March2004.pdf](http://www.unc.edu/[cigar/papers/FileSharing_March2004.pdf)> (draft March 2004):

Downloads have an effect on sales which is statistically indistinguishable from zero, despite rather precise estimates. Moreover, these estimates are of moderate economic significance and are inconsistent with claims that file sharing is the primary reason for the recent decline in music sales.

⁷⁴ *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2004) 205 ALR 319; 59 IPR 299 at [78].

informed of the application. It is respectfully submitted that the orders should not have been granted in this case, and that the developments regarding transitory data not be followed in future.

Scope of order

The Anton Piller orders in this case allowed a very wide range of information to be gathered from Sharman networks, Sharman's Internet Service Providers and several Australian universities whose networks may have been used as supernodes. The definition of relevant information included, significantly:

- Information recording the number or locations of any Australian users, supernodes and central servers;
- Information recording any communication between any Australian servers, supernodes or users;⁷⁵
- Information recording the creation or transfer of any digital music files in Australia through the Kazaa network;
- Information recording digital music files located on the computers of users.

The orders further provided that relevant information could be captured or copied from any 'Electronic Material', and removed into the possession of the applicant's solicitors.⁷⁶ Any 'bitstream' images made, whether of static or dynamic data, were to be kept by the forensic experts present, and were not to be disclosed or analysed without further order of the court.⁷⁷ The parties are still disputing proper access to this information.⁷⁸ Due to unclear drafting of the orders, it is not clear what data should have been kept by the forensic experts, and what could be disclosed to the applicants. The intention was to have all static data treated as discoverable documents and kept by the forensic experts until a later date, while all dynamic (or transitory) data could be analysed by the respondents.⁷⁹

The information gathered pursuant to these orders would necessarily have included records of communications with a large number of individual users. Transitory data is much more telling of an individual's conduct than static data. Assumedly, static data would only concern the data that was recorded by Sharman or its systems, and could be quite tightly controlled to ensure that the privacy of users was not infringed. Dynamic data, on the other hand, includes data that is passing through the system (communications) which necessarily shows all the actions of all the users of the system at the time of observation that passed through Sharman's networks. Many of these communications would concern non-infringing conduct as users interact with the network, for example, searching, communicating with other users, sharing files not covered

⁷⁵ Note that this does not include information recording communications solely between users, because that information would not pass through the systems named by the orders, and the orders did not authorise the collection of data from any user's premises.

⁷⁶ Order 4.

⁷⁷ Orders 13 and 14.

⁷⁸ *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* [2004] FCA 934 (unreported, Wilcox J, 1 July 2004, BC200404427), reported in A Dinham, 'Kazaa copyright trial set for November', CNET News.com, 2 July 2004 <http://zdnet.com.com/2100-1104_2-5255741.html> (accessed 14 July 2004).

⁷⁹ *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2004) 205 ALR 319; 59 IPR 299 at [76].

by copyright, or which are licenced permissively,⁸⁰ or in ways which constitute fair dealing. Some of the information gathered may not even be communication *with* the network, but incidental communication that is caught in the net, in that it passes through the system but for an unrelated purpose.

If the court decided that there was a prima facie case against Sharman, and that the risk of damage and destruction of data was so great that it necessitated granting an Anton Piller order, certainly the order should have been limited to protect the privacy rights of the users of the system, against whom Universal had made no claim.

A civil investigation right

The plaintiffs contended that the information sought would help them to obtain detailed knowledge about the operation of the Kazaa system, including:

the nature and extent of communications passing between various elements of the Kazaa system, including encrypted communications, the content of such communications, and the existence and operation of mechanisms used by the operators, programmers and administrators of the Kazaa system to control or monitor aspects of the system.⁸¹

Setting aside the principle that Anton Piller orders should only be used to preserve data, it is clear that the information sought could be relevant to determining the potential liability of the defendants and users of the system. Relevance on its own, however, should not justify the granting of Anton Piller orders. If this line of reasoning were widely accepted, interested parties could obtain a similar order whenever they suspected that their rights were being infringed, without regard for the privacy rights either of the respondents or, even more importantly, the individuals who will be inevitably caught up in the investigation.

The applicants contended that if the orders were not granted, there was 'likely to be a large number of participants who would seek to conceal themselves'⁸² from any other investigation the applicants would make. This line of reasoning is disingenuous; the fact that individual users would exercise their rights to privacy by not allowing themselves to be monitored if they knew of a monitoring process is not, and can not be, a justification for covert surveillance by private entities. The right to privacy necessarily has limits, and should not protect the concealment of infringing behaviour; but neither should it give way completely to investigations of potential infringing behaviour.

There are a number of ways in which the orders could have been modified to not include data about users, if it was concluded that further information about the operation of the system was necessary to Universal's investigation. The extent of control exercised by the operators of the network could have been discovered by examining the source code of the applications running on

80 For an example of a permissive licensing scheme for digital media, see Creative Commons <<http://creativecommons.org>> (accessed 15 July 2004).

81 *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2004) 205 ALR 319; 59 IPR 299 at [10].

82 *Ibid.*, at [12].

the servers,⁸³ or by obtaining a working copy of the applications running on the servers and hosting a demonstration, or by obtaining preliminary discovery from the respondents and issuing subpoenas to parties likely to know.

By substantially waiving threshold requirements and allowing a private entity to capture and analyse data showing communications involving an enormous amount of individual users, Wilcox J has set an alarming precedent for intellectual property enforcement. The logical extension of this principle is the use of Anton Piller orders to obtain information from parties against whom the applicant has no actual cause of action, or no intention of proceeding against, in order to capture communications between individuals or other third parties involved. This would allow a much greater power to discover infringements and defendants than would otherwise be available through the normal channels for pre-action discovery.

For example, this would allow Anton Piller orders to be made against website owners, ISPs, content hosts and operators of other Internet servers, where it is suspected that some of the users may be infringing intellectual property rights. Such orders would dramatically reduce the level of privacy held by Internet users, destroying the delicate balance between intellectual property enforcement and the rights of individuals to their privacy.

2.2 Equitable identity discovery

In 1973, the House of Lords in *Norwich Pharmacal v Commissioners of Customs and Excise*⁸⁴ revived an equitable remedy for discovery against an innocent third party for the purposes of identifying the proper defendants to a proposed action. Generally, discovery is permissible if:

- There is an identifiable cause of action against the wrongdoer;
- The third party is somehow involved in the execution of the wrong, even unwittingly;
- There is no other reasonable way for the wrongdoer to be identified;
- Discovery is not intended as a fishing expedition, in that most of the material facts are known by the would-be plaintiff, except for the identity of the wrongdoer, and the plaintiff was not seeking to gather evidence of infringements; and
- There is no public policy consideration that would prevent discovery (such as confidentiality or efficiency considerations).

Jurisdiction to make the order in Australia is found in the court's equitable auxiliary jurisdiction.⁸⁵

Identifiable cause of action

The courts will consider the strength of the applicant's case in their discretion to order discovery, in order to protect innocent parties from any undue

⁸³ Orders requiring disclosure of source code are dangerous as proprietary software companies place much value on the code, and it is likely to contain much data that would be covered by trade secret protection.

⁸⁴ [1974] AC 133; [1973] 2 All ER 943.

⁸⁵ *Re Pyne* [1997] 1 Qd R 326.

investigation into their affairs.⁸⁶ It has long been recognised that a ‘bill of discovery must be filed in aid of some proceedings either contemplated or intended, and there must be allegations to that effect: a court of equity did not compel discovery for the mere gratification of curiosity’.⁸⁷

Where the case against the alleged wrongdoers is weak, the courts will generally not allow discovery. In *AXA Equity v National Westminster Bank*, Rimer J noted that ‘in *Norwich Pharmacal* the House of Lords regarded the plaintiffs as having the strongest prima facie case of infringement against the importers’, and refused to grant discovery, partly on the basis that the ‘whole point of [the plaintiffs’] discovery application against the defendants is to find out if they do have a case’.⁸⁸

It is interesting to note that the plaintiff need not actually intend to sue the person to be identified by the discovery — ‘it is sufficient if he has a cause of action (whether or not he intends to pursue it) and that discovery is necessary to enable justice to be done’.⁸⁹

Involvement in the wrong — the ‘mere witness’ rule

In *Norwich Pharmacal*, Lord Reid noted that ‘information cannot be obtained by discovery from a person who will in due course be compellable to give that information either by oral testimony as a witness or on a subpoena duces tecum’.⁹⁰ Discovery is only available against a person who was somehow involved in and facilitated the wrongdoing, even innocently.⁹¹ In most cases dealing with online communications, the mere witness rule will not apply to prevent discovery from service providers — a provider will generally always be considered to have somehow facilitated any wrongdoing of which it has information.⁹²

No other reasonable way to obtain the information

If there is another reasonable way for the wrongdoer to be identified, the courts will not put the respondent to the trouble of discovery. Similarly, if the applicant has been lax or incomplete in its investigations, the discretion will generally not be exercised.⁹³

⁸⁶ See *Glaxo Wellcome PLC v Canada (Minister of National Revenue)* (1998) 81 CPR (3rd) 372 at 387 per Stone JA: ‘the requirement that the appellants have a bona fide claim against the alleged wrongdoers is intended to ensure that actions for a bill of discovery are not brought frivolously or without any justification.’

⁸⁷ E Bray, *The Principles and Practice of Discovery*, Reaves & Turner, London, 1885, p 611.

⁸⁸ *Axa Equity and Law Life Assurance Society v National Westminster Bank* (unreported, Ch Div, Rimer J, 2 February 1998, Transcript: B F Nunnery).

⁸⁹ *Re Cojuango* (1986) 4 NSWLR 513 at 521.

⁹⁰ *Norwich Pharmacal Co v Commissioners of Customs and Excise* [1974] AC 133 at 174A; [1973] 2 All ER 943 at 947 per Lord Reid.

⁹¹ *Ibid*, at 960, per Viscount Dilhorne: ‘it matters not that the involvement or participation was innocent and in ignorance of the wrongdoing.’

⁹² *Ibid*, at 968, where Lord Cross held that since the respondents had effective control of the infringing goods, if not legal possession, they would be under a duty to disclose the names, unless they could claim privilege on the grounds of public interest. See also *Totalise plc v Motley Fool Ltd* [2003] 2 All ER 872; [2001] All ER (D) 213 (Feb) (Owen J, 19 February 2001), *The Times*, 15 March 2001 (Transcript: Smith Bernal).

⁹³ *Eg*, in *BMG Canada Inc v John Doe* [2004] FC 488 (Can Fed Ct, Von Finckenstein J, 31 March 2004), there was no evidence led explaining how the pseudonym username was

No inconsistent public policy considerations

The courts will generally ‘weigh the requirements of justice to the appellants against the considerations put forward by the respondents as justifying non-disclosure’.⁹⁴ For example, the courts will consider whether discovery would conflict with the privilege against self incrimination,⁹⁵ legal professional privilege, public interest privilege,⁹⁶ or whether the discovery is likely to adversely affect the business of the respondent.⁹⁷

It is at this point that the courts should balance the privacy interests of persons affected by the order. While the rights of individuals to their privacy are usually recognised, they are rarely given the emphasis they deserve. It is submitted that the recent approach taken by von Finckenstein J of the Canadian Federal Court is to be favourably applied in Australia. In an action to discover the identity of users of a filesharing network, his Honour considered that in order to grant identity discovery, ‘the public interests in favour of disclosure must outweigh the legitimate privacy concerns’.⁹⁸ This proposition would have the effect of bringing the privacy issues to the forefront of the court’s consideration when exercising the discretion to order discovery.

Discovery is not intended as a fishing expedition

There is some debate as to whether *Norwich Pharmacal* relief is only available to identify possible defendants or, if not, to what extent it can be used to gather evidence against possible defendants. In some ways, this confusion can be seen to be drawn from Lord Reid’s statement that a person involved in a wrong ‘comes under a duty to assist the person who has been wronged by giving him *full information and disclosing the identity* of the wrongdoers’.⁹⁹ A careful reading of the case, however, suggests that the House of Lords did not intend that the order go beyond what was necessary for identifying the wrongdoers. Indeed, Lord Cross acknowledged fears that the court might be ‘opening the door to “fishing requests” by would-be plaintiffs’.¹⁰⁰ His Honour dismissed those fears, noting that ‘there is a clear

linked to an IP address, and von Finckenstein J considered at [20] that ‘without being satisfied that such evidence is reliable, it would be irresponsible for the court to order the disclosure of the name of the account holder of [the IP address] and expose this individual to a law suit by the plaintiffs’.

94 *Norwich Pharmacal Co v Commissioners of Customs and Excise* [1974] AC 133 at 175F; [1973] 2 All ER 943 at 949 per Lord Reid; see also *Alfred Crompton Amusement Machines v Customs & Excise Commissioners (No 2)* [1974] AC 405 at 433D per Lord Cross; [1973] 2 All ER 1169: ‘In a case where the considerations for and against disclosure appear to be fairly evenly balanced the courts should I think uphold a claim to privilege on the ground of public interest’.

95 *Rank Film Distributors Ltd v Video Information Centre* [1982] AC 380; [1981] 2 All ER 76.

96 *R v Lewes Justices; Ex parte Secretary of State for Home Department* [1973] AC 388; *Sankey v Whitlam* (1978) 142 CLR 1; 21 ALR 505.

97 *Sega Enterprises Ltd v Alca Electronics Ltd* [1982] FSR 516.

98 *BMG Canada Inc v John Doe* [2004] FC 488 (Can Fed Ct, von Finckenstein J, 31 March 2004) at [13].

99 *Norwich Pharmacal Co v Commissioners of Customs and Excise* [1974] AC 133 at 175B; [1973] 2 All ER 943 at 948 per Lord Reid (emphasis added).

100 *Ibid.*, at AC 199D; All ER 969.

distinction between simply asking for the name of a person whom you wish to make a defendant and asking for evidence'.¹⁰¹

Lord Reid's statement was considered in *Arab Monetary Fund v Hashim (No 5)*, where Hoffmann J said:

The reference to 'full information' has sometimes led to an assumption that any person who has become 'mixed up' in a tortious act can be required not merely to disclose the identity of the wrongdoer but to give general discovery and answer questions on all matters relevant to the cause of action. In my view this is wrong. The principle upon which Lord Reid distinguished the 'mere witness' rule was that unless the plaintiff discovered the identity of the wrongdoer, he could not commence proceedings. The reasoning of the other members of the House is the same. The *Norwich Pharmacal* case is no authority for imposing upon 'mixed up' third parties a general obligation to give discovery or information when the identity of the defendant is already known.¹⁰²

In *McLean v Burns Philp Trustee*,¹⁰³ Young J also held that *Norwich Pharmacal* did not provide any authority to order discovery of documents not relating to the identity of alleged wrongdoers.

Two well known cases are often cited as authority for a wide ranging *Norwich* order. In *Bankers Trust Company v Shapira*,¹⁰⁴ the plaintiffs sought discovery against a bank in order to trace money that had been fraudulently obtained by the defendants, who were known to, and had been sued by, the plaintiffs. Lord Denning MR relied on *Norwich Pharmacal* to make a wide order for discovery. Some time later, in *Mercantile Group v Aiyela*,¹⁰⁵ the Court of Appeal made a discovery order against the wife of a defendant in aid of a post-judgment Mareva injunction, again relying on *Norwich Pharmacal* as authority for the order. The principles linking these three cases were cogently explained by Rimer J in *AXA Equity v National Westminster Bank*, where his Honour noted that all three cases provide examples of exceptions to the 'mere witness' rule, and not an extension of the identity discovery principle.¹⁰⁶ His Honour then continued to deal with the specific claim in the case before him:

[The Plaintiff's] argument is, in effect, that there is a further exception, namely the case where, although the alleged wrongdoer has been identified, there will be no trial unless the desired discovery is obtained since without it the plaintiffs will not know if they have a case at all, cannot therefore plead it and cannot progress it to trial. In my judgment, however, there is no such further exception. For reasons given earlier,

101 Ibid.

102 [1992] 2 All ER 911 at 914B.

103 (1985) 2 NSWLR 623 at 645.

104 [1980] 3 All ER 353.

105 [1994] QB 366; [1994] 1 All ER 110.

106 *Axa Equity and Law Life Assurance Society v National Westminster Bank* (unreported, Ch Div, Rimer J, 2 February 1998, Transcript: B F Nunnery): 'The defendants against whom they seek discovery are, in principle, compellable to give evidence at any trial so that, on the face of it, the discovery order sought against them infringes the mere witness rule and cannot therefore be made. There are exceptions to the mere witness rule, of which *Norwich Pharmacal* provides one type of example, and the *Bankers Trust* and *Aiyela* cases provide others'.

I consider that applications for discovery for that purpose are in the nature of ‘fishing’ applications which the court will not allow.¹⁰⁷

In *Corrs Pavey Whiting Byrne v Collector of Customs*,¹⁰⁸ Gummow J, in a dissenting judgment, noted that seeking evidence to found an action would go beyond the principles in *Norwich Pharmacal*, but may be justified on the basis of growing US authority ‘that the jurisdiction extends beyond discovery of names and addresses of prospective defendants’.¹⁰⁹ His Honour did not need to decide further whether such disclosure was justified in that case. Likewise, in 1999, the Full Court of the Federal Court noted the different approaches but left the issue open.¹¹⁰

The golden thread in these judgments appears to be that in some cases, a non-party may be required to give discovery which goes beyond the identity of a wrongdoer, in order to ensure that justice is done.¹¹¹ These cases act as further exceptions to the ‘mere witness’ rule; a person who would otherwise not be compellable to disclose information until a trial is underway can be compelled to do so if justice requires it, for example by allowing money to be traced when a Mareva order is made,¹¹² or tracing breaches of confidence to prevent imminent damage to the plaintiff’s market share.¹¹³

It is submitted that these judgments do not provide authority for widening the discovery available under a *Norwich Pharmacal* order — when an order is made for identity discovery, it should not be extended to allow a plaintiff to fish for information about the potential liability of any unknown wrongdoers.¹¹⁴

¹⁰⁷ Ibid.

¹⁰⁸ (1987) 14 FCR 434; 74 ALR 428.

¹⁰⁹ Ibid, at FCR 446; ALR 440.

¹¹⁰ *Hooper v Kirella Pty Ltd* (1999) 96 FCR 1; 167 ALR 358 at [28].

¹¹¹ See, for example, *McLean v Burns Philp Trustee* (1985) 2 NSWLR 623 at 646: ‘It is, of course, unwise to restrict the court’s inherent power to order discovery to the *Norwich* type situation or cases that would have been covered by the old bill of discovery procedure. The power clearly extends further. . . . The Court may order discovery in relation to a claim for final relief so that that claim can be dealt with properly and justly’.

¹¹² *Mercantile Group (Europe) AG v Aiyela* [1994] QB 366; [1994] 1 All ER 110.

¹¹³ *Computershare Ltd v Perpetual Registrars Ltd* (2000) 1 VR 626 at [19] per Warren J: ‘If Computershare was compelled to await trial before the information was revealed to it it may well be too late as its dominance in the market place in the provision of its services would be undermined and, further, the value of its next generation software could be totally diminished’.

¹¹⁴ This position was enunciated by Hofman LJ in *Mercantile Group (Europe) AG v Aiyela* [1994] QB 366 at 374G; [1994] 1 All ER 110 at 115:

Mr Mann says that the *Norwich Pharmacal* principle is limited to finding out the identity of a tortfeasor. But this is not the only situation which falls outside the mere witness rule. In *Bankers Trust Co v Shapira* [1980] 1 WLR 1274 discovery was ordered against a bank which had received the proceeds of fraud. The purpose of discovery was to trace what had happened to the money. The bank had innocently become mixed up in the fraud and there was no infringement of the mere witness rule because there would be no point in the plaintiff seeking the information at the trial. By that time the money would be gone. In *A v C* (Note) [1981] QB 956, 961, Robert Goff J made an order for disclosure in aid of a pre-judgment Mareva against a bank which had been joined solely for the purposes of discovery.

This passage was referred to with apparent approval by Gummow J in *Breen v Williams* (1996) 186 CLR 71 at 120; 138 ALR 259. Cf *P v T Ltd* [1997] 4 All ER 200; [1997] 1 WLR

2.3 Pre-action discovery under the rules of the court

In some Australian jurisdictions, preliminary discovery is regulated by the rules of the court. The rules generally draw a distinction between identity discovery, along the *Norwich Pharmacal* principles, and information discovery, which allows wider discovery in order to investigate a possible cause of action, but only against a potential respondent. In this section we will mainly discuss the Federal Court Rules, and any significant differences will be cited.

Identity discovery

Identity discovery has been incorporated into the Federal Court Rules (FCR) and the rules of the court of the supreme courts of New South Wales, Victoria, the Australian Capital Territory and the Northern Territory.¹¹⁵ The South Australian rules do not provide for identity discovery, but have been used to identify further respondents.¹¹⁶ Queensland, Tasmania and Western Australia do not have statutory preliminary discovery rules.

Under FCR O 15A r 3, identity discovery will generally be allowed:

Where an applicant, having made reasonable inquiries, is unable to ascertain the description of a person sufficiently for the purpose of commencing a proceeding in the Court against that person . . . and it appears that some person has or is likely to have knowledge of facts, or has or is likely to have or has had or is likely to have had possession of any document or thing, tending to assist in such ascertainment.

Statutory identity discovery is much the same as under the *Norwich Pharmacal* principle, save that the threshold tests appear to be significantly lower. In cases against ISPs or content hosts, it will often be the case that a potential litigant will be able to satisfy the tests expressed in the rule. The rule is available even if the respondent is a 'mere witness' or a bystander,¹¹⁷ allowing discovery against any entity on the Internet who is in a position to identify an alleged wrongdoer. More importantly, the applicant is not required to show a *prima facie* case against the prospective respondent.¹¹⁸ The courts will not make the order to allow the applicant to commence 'merely speculative proceedings'¹¹⁹, but the required level of proof is much lower than under the *Norwich Pharmacal* rule.

The rules are widely phrased to allow flexibility and prevent arbitrary inhibitions on the court's discretion. That discretion, then, must act as the

1309 (Sir Richard Scott V-C); *Corrs Pavey Whiting & Byrne v Collector of Customs (Vic)* (1987) 14 FCR 434 at 445–6 per Gummow J; 74 ALR 428.

115 FCR O 15A r 3; Supreme Court Rules 1970 (NSW) Pt 3; General Rules of Procedure in Civil Proceedings 1996 (Vic) r 32.03; Supreme Court Rules (ACT) O 34A; Supreme Court Rules 1987 (NT) r 32.03.

116 Supreme Court Rules 1987 (SA) r 60.01; see *State Bank of South Australia v Hellaby* (1992) 59 SASR 304.

117 *Stewart v Miller* [1979] 2 NSWLR 128 at 135 per Sheppard J. This was a decision concerning the equivalent New South Wales rule. The principle was endorsed with regard to r 3 by the Full Federal Court in *Hooper v Kirella Pty Ltd* (1999) 96 FCR 1; 167 ALR 358 at [32].

118 *Levis v McDonald* (1997) 75 FCR 36 at 41, 44; 155 ALR 300; approved of in *Hooper v Kirella Pty Ltd* (1999) 96 FCR 1; 167 ALR 358 at [33].

119 *Stewart v Miller* [1979] 2 NSWLR 128 at 140.

brake on the exercise of this power.¹²⁰ In exercising the discretion, the courts will take into account the prospects of the applicant's success before granting an order.¹²¹ The court must further take into account public policy considerations — the applicant must show that 'the order sought is necessary in the interests of justice; in other words, the making of the order is necessary to provide [the applicant] with an effective remedy in respect of the actionable wrong of which he complains'.¹²² In the past, this has been particularly relevant to the 'newspaper rule', which balanced a plaintiff's grievances with the public interest in preserving the anonymity of journalistic sources. It is submitted that the public interest in preserving the anonymity of individuals on the Internet should also be recognised and balanced in the same way.

The type of information that is discoverable under the rules extends only to the description of a person for the purpose of commencing a proceeding.¹²³ Information discovered should not extend to information discovery. In the Federal Court and the ACT Supreme Court, the rules provide for much wider discovery to be ordered, which may extend the scope of information discovered, as we will see below.¹²⁴

Information discovery from prospective respondent

In the Federal Court, Victoria, the Australian Capital Territory and the Northern Territory, the rules of the court provide for information discovery from a prospective respondent.¹²⁵

Rule 6 of the FCR provides:

where:

- (a) there is reasonable cause to believe that the applicant has or may have the right to obtain relief in the Court from a person whose description has been ascertained;
- (b) after making all reasonable inquiries, the applicant has not sufficient information to enable a decision to be made whether to commence a proceeding in the Court to obtain that relief; and
- (c) there is reasonable cause to believe that that person has or is likely to have or has had or is likely to have had possession of any document relating to the question whether the applicant has the right to obtain the relief and that inspection of the document by the applicant would assist in making the decision;

the Court may order that that person shall make discovery to the applicant of any document of the kind described in paragraph (c).¹²⁶

Interestingly, these rules are available where the applicant has already established a *prima facie* case, but still does not have enough information to

¹²⁰ *Paxus Services Ltd v People Bank Pty Ltd* (1990) 99 ALR 728; 20 IPR 79.

¹²¹ *Exley v Wyong Shire Council* (unreported, NSW SC, Master Allen, 10 December 1976), cited in *Hooper v Kirella Pty Ltd* (1999) 96 FCR 1; 167 ALR 358 at [33].

¹²² *John Fairfax & Sons Ltd v Cojuangco* (1988) 165 CLR 346 at 357; 82 ALR 1.

¹²³ FCR O 15A r 1; NSW Pt 4 r 1 (3); Vic r 32.01; ACT O 34A r 1; NT r 32.01.

¹²⁴ FCA O 15A r 12; ACT O 34A r 8.

¹²⁵ FCR O 15A r 6; General Rules of Procedure in Civil Proceedings 1996 (Vic) r 32.05; Supreme Court Rules (ACT) O 34A r 5; Supreme Court Rules 1987 (NT) r 32.05.

¹²⁶ The ACT rule does not require the right to relief to be based in the ACT Supreme Court (ACT O 34A r 6(a)), nor does it require 'all reasonable inquiries', but only 'reasonable inquiries' to be made (ACT O 34A r 6(b)).

make a decision as to whether to proceed with the case.¹²⁷ This means that information relating to the flagrancy of any infringements, or as to any possible defences, will generally be discoverable.¹²⁸ This may be used as a ground for disclosing the activities of third parties. The rule will not, however, be available after substantive proceedings have been instituted.¹²⁹

Information discovery is available 'only against the person in respect of whom there is reasonable cause to believe that the applicant has or may have the right to obtain relief in the court'.¹³⁰ Again, it is not necessary to demonstrate a prima facie case, but the applicant must do more than phrase his or her case in terms of the conditions for infringement.¹³¹

These rules should not be available to gather information from third parties. However, where a third party can be implicated in an infringement, for example by attracting secondary liability by allegedly authorising that infringement, discovery may be allowed.¹³² This discovery is potentially wide ranging, including information on the activities of users, where that information is known by the third-party or somehow passes through its systems.¹³³ Effectively, then, this means that discovery can be sought about the actions of an individual from a third party, where that third party can be shown to attract some potential liability. The House of Lords in *Norwich Pharmacal* were quite critical of this same suggestion in relation to the 'mere witness' rule.¹³⁴ Indeed, it would seem quite illogical that a plaintiff would be

127 *Alphapharm Pty Ltd v Eli Lilly Australia Pty Ltd* [1996] FCA 391 (unreported, Lindgren J, 24 May 1996, BC9602085) at 33. The test is an objective one: at 31.

128 *Hooper v Kirella Pty Ltd* (1999) 96 FCR 1; 167 ALR 358 at [40].

129 *Ricegrowers Co-operative Ltd v ABC Containerline NV* (1996) 138 ALR 480 at 484 per Tamberlin J.

130 *Hooper v Kirella Pty Ltd* (1999) 96 FCR 1; 167 ALR 358 at [36].

131 See *Minister for Health & Aged Care v Harrington Associates Ltd* [1999] FCA 549 (unreported, 4 May 1999, BC9902167) at [28] per Sackville J: 'FCR O 15A, r 6(a) poses an objective test, namely, whether there is reason to believe that the applicant has or may have the right to obtain relief from a person whose description has been ascertained'. See also *CCA Beverages (Adelaide) Ltd v Hansford* [1991] FCA 925 (unreported, 15 November 1991, O'Loughlin J, BC9102965) at 12; *Viskase Corp v Cryovac Inc* [2000] FCA 1695 (unreported, 22 November 2000, BC200008617).

132 *Sony Music Entertainment (Australia) Ltd v University of Tasmania* (2003) 129 FCR 472; 198 ALR 367.

133 *Sony Music Entertainment (Australia) Ltd v University of Tasmania* [2003] FCA 724 (unreported, Tamberlin J, 18 July 2003, BC200303853).

134 *Norwich Pharmacal Co v Commissioners of Customs and Excise* [1974] AC 133 at 195B; [1973] 2 All ER 943 at 966; Lord Cross considered that it would be illogical to constrain a plaintiff's right to discovery to a question of 'whether or not the plaintiff could have obtained some relief against the defendant if he had chosen to ask for it':

Per Lord Reid at 947: 'To apply the mere witness rule to a case like this would be to divorce it entirely from its proper sphere. Its purpose is not to prevent but to postpone the recovery of the information sought. It may sometimes have been misapplied in the past but I see no reason why we should continue to do so'.

Per Viscount Dilhorne at 958: 'It would indeed be odd if you could get discovery if you named the party you intended to sue if you could discover his responsibility, but that you could not get discovery though you had suffered an injury if you were not able to name the person who might be responsible'.

Per Lord Kilbrandon at 974: 'the liability of the defendant in discovery to be sued . . . as I have said, had in my view no bearing on the liability to discovery in a suit proposed to be brought against a third party'.

able to obtain information about a possible defendant's actions from a third party only where there was a possible cause of action against that third party, even if the plaintiff never intended to pursue that cause of action.

A cogent distinction may lie where the person against whom discovery is sought shares liability with other persons, in a wrongful act or series of wrongful acts in which they are all involved. In *Kirella v Hooper*,¹³⁵ after ordering identity discovery under FCR O 15A r 3, Tamberlin J also ordered information discovery under r 6, on the basis that:

[the applicant] is also entitled to have sufficient information to decide whether it has the right to obtain relief against additional persons or entities who may be involved, particularly where there is some indication of a concerted course of conduct among a number of persons and entities over a period of months, as in the instant case.¹³⁶

It is suggested that this distinction means that combined identity and information discovery may be available against a group of joint tortfeasors, but not against a person with little or no liability with a view to identifying, and uncovering information on, a mostly unrelated wrongdoer.¹³⁷

Inspection and preservation of property

Under FCR O 15A r 12 and Supreme Court Rules (ACT) O 34A r 8, the court may also make an order for the 'inspection, measurement, photocopying, preservation, custody and detention'¹³⁸ of property relevant to proceedings, or the taking of samples, observation, carrying out of any experiment, 'making, playing or screening of tape recordings and films and other means of recording sight or sound' or 'making and reproducing or displaying other instrumental recordings and tracings' with respect to such property.¹³⁹

The wide wording of these rules makes it clear that the court has a wide discretion to order extra discovery as appropriate in an application for preliminary discovery. The primary concern with these provisions is that they may allow access to a wider range of data than is necessary under each rule. There is some uncertainty as to whether an order under FCA O 15A r 12 is available only when some other preliminary discovery has been ordered under O 15A, or if it can be ordered on any application under the order, thus enlarging the type of discovery available under the other rules. O'Loughlin J in *CCA Beverages (Adelaide) v Hansford*¹⁴⁰ considered that an order under r 12 could be made only if an order had already been made for 'pre-action' discovery. Conversely, in *Pacific Dunlop v Australian Rubber Gloves*,¹⁴¹ Heerey J held that the court had power 'to make an order for inspection whenever any application is made under O 15A, irrespective of whether any other order is made'.¹⁴²

135 [1999] FCA 1839 (unreported, Tamberlin J, 23 December 1999, BC9908555).

136 Ibid.

137 See, for example, *Computershare Ltd v Perpetual Registrars Ltd* (2000) 1 VR 626, where the exchange (the third party) was not a very distant third party, being prepared to spend \$50m in a joint venture, amongst other things).

138 Order 15A r 12(a).

139 Order 15A r 12(b)(i)-(v).

140 [1991] FCA 925 (unreported, O'Loughlin J, 15 November 1991, BC9102965).

141 (1992) 23 IPR 456.

142 Ibid, at 467.

Kremer and Davies suggest that the wider view is to be preferred, and 'the words in r 12 should be read distributively, adding the power to order the specified relief to each of r 3 and r 6'.¹⁴³ If this is the case, I would respectfully suggest that such an order must still be made for the purposes of r 3 or r 6, and should not go further than what is reasonably required under those rules. That is, in an application for identity discovery, inspection or preservation of property may be required in order to identify a defendant, but the information disclosed should not exceed what is reasonably necessary for that purpose, and should not amount to information discovery.

Blurring the distinctions: *Sony v University of Tasmania*

In *Sony v University of Tasmania*,¹⁴⁴ Sony sought preliminary discovery under FCR O 15A rr 3, 6 and 12, against three Australian universities. There appeared to be some copyright music files on some of the universities' file servers, including files made available through a small number of users' personal web space. Sony sought to have the file servers' backup media discovered. These backup media contained home directories, web spaces, email spools and any other data stored on the relevant servers. The universities sought to have the scope of documents discovered limited to files whose names matched against certain rudimentary patterns associated with digital media files and music recordings, as well as the email spools belonging to the named users.

Interestingly, it seems that Sony never intended to proceed against the universities, but still sought information discovery under r 6. Tamberlin J acknowledged that identity discovery under r 3 provided a limitation on the court's power such that 'the court may only discover a closed category of documents where the judgment is for the respondents and their solicitors, and not for the applicants or even for the court, as to whether the documents relate to the description of the person concerned'.¹⁴⁵ However, his Honour considered that the information that would normally be irrelevant under r 3 was still relevant 'in relation to other persons who may have been in electronic correspondence with them',¹⁴⁶ such that 'it could also be necessary to know the identity of such persons for the purpose of description'.¹⁴⁷ The argument here is that in order to identify someone under r 3, an applicant will need information discovery (of the type available under r 6) to first identify any wrongdoings. This seems incongruous with the purpose of identity discovery as we have seen so far; without some evidence of infringement by any unknown entities, discovery is generally not available, either under the equitable principles or the statutory discovery rules.

Justice Tamberlin considered that if 'the narrow search tools and methods proposed by the universities . . . are used, then it is likely that there will be insufficient discovery'.¹⁴⁸ His Honour noted that the court had wide discretion

143 B Kremer and R Davies, 'Preliminary discovery in the Federal Court: Order 15A of the Federal Court Rules' (2004) 24 *Aust Bar Rev* 235.

144 (2003) 129 FCR 472; 198 ALR 367.

145 *Ibid.*, at [43].

146 *Ibid.*

147 *Ibid.*

148 *Ibid.*, at [63].

to make orders under O 15A, and considered that the exercise of that discretion would depend upon the balance of the public interest.

His Honour considered that the ‘important public interest in protecting the privacy of those using university facilities, particularly where the discovery process may disclose totally irrelevant personal information concerning a wide range of individuals and entities’¹⁴⁹ would be largely resolved by imposing express undertakings preventing the ‘misuse or abuse of information given on discovery and its use for purposes other than in the proceeding in which discovery was ordered’.¹⁵⁰

This case highlights the flexibility inherent in the discretion to order preliminary discovery. It also blurs the distinction between identity discovery in r 3 and information discovery in r 6. The court appeared to hold that the discretion available in the rules of O 15A enabled a wide public interest balancing test to be applied when determining what level of discovery should be allowed:

Another matter to be weighed in balancing the factors in the exercise of discretion is the *public interest in having full and proper disclosure* by way of preliminary discovery in order to ensure that an informed decision can be made as to *whether to commence proceedings and against whom they should be brought*.¹⁵¹

The information made available on discovery was much greater than Sony needed to either ‘ascertain the description of a person sufficiently for the purpose of commencing a proceeding’,¹⁵² or to ascertain whether it ‘has or may have the right to obtain relief in the court’¹⁵³ (from the universities). It is clear that the information sought must have included much information that was clearly irrelevant to the case on the evidence put forward by Sony, including the personal data of many users.¹⁵⁴ Again, as we saw in *Universal v Sharman*,¹⁵⁵ this type of information extends to the question of whether Sony has the right to obtain relief against *individual users*, not the third party against whom it has obtained discovery.

The applicants put forward evidence that showed that there were ‘at least two sound recordings’¹⁵⁶ on a university server. On this evidence, a valid preliminary discovery request would allow Sony to obtain information showing the identity of the person who was responsible for those infringing sound recordings, under r 3. Another valid application could be sought against that identified person, under r 6, which could reveal sources of the infringing media and show whether other persons were involved in the acts or related acts of infringement. A further valid application could have been sought against the universities, to see if they were responsible for the infringing

149 Ibid, at [64].

150 Ibid, at [64].

151 Ibid, at [65] (emphasis added).

152 FCR O 15A r 3.

153 FCR O 15A r 6.

154 *Sony v University of Tasmania* (2003) 198 ALR 367 at [62]: ‘The evidence of the witnesses . . . persuades me that . . . some relevant material is likely to be recovered but such recovery will include a great deal of extraneous and irrelevant material’.

155 *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2004) 205 ALR 319; 59 IPR 299.

156 *Sony v University of Tasmania* (2003) 198 ALR 367 at [27].

material or whether they had ‘authorised’ the infringement, but without disclosing information as to any users’ identity or other private information. It does not follow that the applicants could legitimately use somewhat controversial forensic data recovery techniques¹⁵⁷ to see if there was any evidence of any other *unrelated* infringing acts. Yet this was the end result of the application — the backup media were handed over to forensic investigators, on an undertaking of confidentiality, and only after that process were the universities able to go through the data and make decisions on privileged documents.

This case provides an alarming example of the growing trend to make wide orders for discovery of computerised records. The court in this case has in effect condoned a large scale fishing expedition through an intermediary’s records in order to determine if there had been any infringements of copyright and, if so, by whom.

3 Restoring the balance — considering the privacy interests of affected parties

When courts are considering applications to disclose private information from intermediaries, the privacy rights of the individuals concerned must be carefully balanced with the rights of the applicant. In most cases for preliminary third party discovery, the individuals whose privacy is to be set aside are not represented before the court. Accordingly, the court must take extra care in examining the potential effect of the proposed disclosure on those individuals. Failure to do so means that the task of protecting an individual’s privacy falls solely on a disinterested intermediary, and the rights of the individual are relegated to a more inconvenient and costly procedure to be taken after the disclosure (and damage) has occurred.

In *Sony v University of Tasmania*, Tamberlin J recognised that the persons whose privacy was affected were the individual users of the university systems,¹⁵⁸ but failed to make a detailed consideration of when it would be permissible to reveal their personal information to a forensic expert (and subsequently, the applicants). It is submitted that courts should take considerable care to tailor discovery to a level that is appropriate with respect to those persons whose privacy will most likely be affected, rather than allowing wide discovery on the grounds that the information is available or that the technology involved is novel or unfamiliar. Unfortunately, this may add some time to the application process as a more detailed investigation into the technology and affected individuals will be required.

3.1 Restructuring the threshold tests

Having recognised that it is the users’ privacy which is primarily infringed in third party discovery cases against intermediaries, some consideration must be given to the threshold tests that must be satisfied before discovery is granted.

¹⁵⁷ See, generally, A McCullagh and W Caelli, ‘Extended case note and commentary: *Sony Music Entertainment (Australia) Limited & others v University of Tasmania & others* [2003] FCA 532’, (September 2003) 53 *Computers & Law* 16.

¹⁵⁸ (2003) 198 ALR 367 at [64].

In Anton Piller applications, a strong prima facie case must be shown against the intermediary only. If significant private information on the intermediary's users is to be subject to the order, then it is submitted that a prima facie case must be demonstrated against those persons too.

In cases like *Universal v Sharman*,¹⁵⁹ this could mean that before seizing records of all communications with users, the plaintiffs would have to show a prima facie case against each user, or at least against a large proportion of users. This requirement would make a wide ranging order much more difficult to obtain, but could be justifiable on the basis that it would force consideration of the rights of all affected parties, discourage the use of Anton Piller orders as investigation tools, and, most importantly, encourage applicants to devise methods of obtaining any necessary data without infringing the privacy rights of third parties.

Legitimising fishing

The statutory rules go some way to legitimising 'fishing' in pre-action discovery.¹⁶⁰ In *Paxus Services Ltd v People Bank Pty Ltd*,¹⁶¹ Burchett J noted that the FCR, as remedial delegated legislation, were to be interpreted liberally. The discretion of the court is the appropriate brake that is to be applied to the otherwise wide power described in the rules.¹⁶² His Honour also noted that:

It is no answer to the applicant's application under r 6 to say that the proceeding is in the nature of a fishing expedition. . . . Rule 6 is designed to enable an applicant, in a situation where his proof can rise no higher than the level the rule describes, to ascertain whether he has a case against the prospective respondent — ie to 'fish' in the old sense.¹⁶³

Similarly, in *Ecologic Holdings Pty Ltd v Hopley*,¹⁶⁴ which concerned particular discovery under FCR O 15 r 8, Nicholson J allowed discovery of documents that were 'likely to have been produced',¹⁶⁵ on evidence which the respondents contended was mere speculation on the basis of their existence and subject matter.

It is suggested, however, that the rules legitimise fishing in the sense that they prevent a potential defendant from remaining silent and avoiding liability. It is not clear that they legitimise fishing in the sense that a potential plaintiff now has a private investigation right to go through the records of any person to identify any wrongdoings of any other person.¹⁶⁶

If the courts have lowered the threshold for discovery to allow 'fishing' in

¹⁵⁹ (2004) 205 ALR 319; 59 IPR 299.

¹⁶⁰ *SmithKline Beecham plc v Alphapharm Pty Ltd* [2001] FCA 271 (unreported, Finklestein J, 19 March 2001, BC200101026) at [19].

¹⁶¹ (1990) 99 ALR 728; 20 IPR 79.

¹⁶² *Ibid.*, at ALR 733 per Burchett J: 'The proper brake on any excesses in its use is the discretion of the court, which is required to be exercised in the particular circumstances of each case'.

¹⁶³ *Ibid.*

¹⁶⁴ [2004] FCA 16 (unreported, RD Nicholson J, 20 January 2004, BC200400025).

¹⁶⁵ *Ibid.*, at [8].

¹⁶⁶ See, for example, *Prosnow International Pty Ltd v Polar Technologies Pty Ltd* (1997) 39 IPR 369 at 374 per O'Loughlin J: 'Nevertheless, that does not mean that an inquirer, properly labelled 'a busy body' should be permitted to make use of these procedures'.

order to facilitate access to justice, bring down the costs of proceedings and prevent the bringing of speculative suits,¹⁶⁷ care must be taken when applying the principle to preliminary third-party discovery. In preliminary discovery actions, respondents are usually afforded a chance to respond, and can put the applicant to proof to show that the application is not an arbitrary investigation into their private affairs.¹⁶⁸ When we consider preliminary discovery against a third-party, designed to seek out information about an alleged wrongdoer, it is that alleged wrongdoer's privacy which is primarily injured, not that of the respondent. Such a procedure can bear some similarity to an *ex parte* application, in that the party responding to the application is potentially disinterested in the result of the application, which makes it difficult for the court to correctly determine the appropriate balance between the enforcement of the applicant's rights and the privacy of any unrepresented persons.

Accordingly, it is suggested that when an order is sought that would interfere with the privacy of individuals not party to the proceedings, the required threshold tests should not legitimise fishing to the extent that it would constitute an injustice to those individuals; an onus should remain on an applicant to show that there is an objective, reasonable belief that some reasonably identifiable cause of action exists, and that the information sought would not go further than is necessary to properly identify the alleged wrongdoers.

3.2 The distinction between identity and information discovery

Preliminary discovery exists to counter the potential injustice where a person who has been wronged does not have access to enough information to bring an action against another party. The important public policy consideration that justice be done must be balanced at all times against the rights of uninvolved parties to their privacy. Accordingly, preliminary discovery is always available as a discretionary remedy, not as by right. Where an applicant can show a cause of action, but not identify a wrongdoer, identity discovery should be granted to allow the applicant to proceed in an action against the correct defendant. Where an applicant does not have sufficient information to show a cause of action, but knows the identity of the alleged wrongdoer, it is sometimes permissible to allow discovery of information that can confirm that cause of action. Information and identity discovery perform different roles, and should not be confused or granted simultaneously. Information discovery has a much lower threshold, but will only affect a small number of named parties, who are afforded an opportunity to contest the application. Identity discovery, on the other hand, can potentially affect a large number of persons, all of whom necessarily have no right of response to the application, but has a much higher threshold. In this way, the process of preliminary discovery is regulated to prevent significant abuse of process.

Where an applicant has neither sufficient information to found a cause of

¹⁶⁷ *Mercantile Mutual v Household Financial Services* (1997) VSCA (unreported, Winneke P, Hayne JA and Ashley AJA, 22 May 1997, BC9702240) which dealt with the Victorian rule.

¹⁶⁸ See *C7 Pty Ltd v Foxtel Management Pty Ltd* [2001] FCA 1864 (unreported, Gyles J, 21 December 2001, BC200108239) at [50].

action, nor to identify a wrongdoer, discovery should not be granted. The case for discovery should not be able to be built from its own bootstraps — the higher threshold for identity discovery should not be able to be satisfied by the information that is proposed to be sought through information discovery. This principle is especially important now that the ‘mere witness’ rule, which previously prevented discovery against uninterested bystanders, has lost much of its significance.¹⁶⁹ As we have already seen, *Sony v University of Tasmania*¹⁷⁰ provides an important example of where the distinction between identity and information discovery has been blurred to the extent that it is practically indistinguishable.

To allow combined information discovery and identity discovery, against generally uninterested persons, is really allowing for a civil investigation right, and fails to properly balance the public interest in potential litigants having the information they require with the public interest that persons be protected from unwarranted investigation into their affairs.

3.3 Limiting the scope of identity discovery

When obtaining identity discovery against an online intermediary, there is often the potential that the identities of a very large number of people will be disclosed. It is difficult for a court, when faced with such an application, to ensure that the discovery will result in only the relevant persons’ identity being disclosed.

For example, in *Sky Channel v Palmer*,¹⁷¹ a *Norwich Pharmacal* order was granted to, among other things, identify suppliers and customers of decoder boxes. Sections 135AN and 135AS of the Copyright Act 1968 (Cth) make it an infringement and an offence respectively to sell, let for hire or distribute broadcast decoding devices. Section 135ANA makes it an infringement to use such a broadcast decoding device for commercial purposes. It is not an infringement for a person to acquire a decoding device, nor is it an infringement to use one for non-commercial purposes. It may be legitimate for a plaintiff to seek to identify commercial users of such devices from the supplier. The difficulty arises when the proportion of non-infringing users is not ascertained at the time the order is made. Perhaps it is legitimate to allow an applicant to trawl through lists of persons to whom such a device was supplied in order to identify any persons who have or are likely to have used the devices in a commercial context. On the other hand, perhaps it is not appropriate to provide extensive listings of all customers of such devices to an applicant who may not have any legal action available against them, but will certainly have an interest in identifying them, if only in order to use other means to dissuade the non-infringing users from engaging in a legal activity.

It is obvious that there is great public interest in not having the identity of unrelated parties unnecessarily disclosed. Again, it is submitted that when exercising the discretion to grant discovery, the courts should consider the real

¹⁶⁹ The statutory discovery rules do not require that the person against whom discovery is sought be involved in the wrong. Even if the equitable remedy has not also been similarly relaxed, anyone on the Internet who is privy to information (without having intercepted it) will generally have ‘facilitated’ any wrongdoing that information concerns.

¹⁷⁰ (2003) 198 ALR 367.

¹⁷¹ [2003] FCA 1246 (unreported, Lindgren J, 31 October 2003, BC200306690).

effect that discovery will have on all the persons involved. If the level of damage claimed is very high, or the possibility that the persons to be named are not wrongdoers is very low, then identity discovery should be granted. On the other hand, where many unrelated persons are at risk of losing their anonymity, the public interest in protecting those persons may outweigh the interest in having the relevant information provided to the applicant. If possible, the order for disclosure should be specific enough that it enables the intermediary to disclose the identity of only those persons against whom the applicant has a prima facie case. This is, of course, usually only possible with a greater level of understanding of the technologies involved than is currently evident.¹⁷²

3.4 Distinguishing information preservation from preliminary discovery

Anton Piller orders are designed to preserve information that will be required in a trial from being destroyed by the respondent, and should not be used as a substitute for preliminary discovery.¹⁷³ It is suggested that the best way to ensure both that potential evidence is preserved and an applicant can obtain information that is necessary to commence an action would involve two separate applications. The first application, which would be made ex parte, would seek preservation only of information; based upon a justified risk of destruction of evidence, an applicant could be granted an Anton Piller order to capture the information required, without examining it. The second application could be made inter partes, because there would be no more risk of evidence being destroyed, and could proceed like a normal preliminary discovery application. As has been seen, this procedure was partially followed in *Universal v Sharman*,¹⁷⁴ where Wilcox J made an order that all bitstream images of electronic information were to be delivered up to the court without further examination by Universal, where they would later be subject to discovery. Unfortunately this requirement was not designed to extend to 'transitory' information, which will be discussed later.

3.5 Restricting the scope of electronic information discovery

The range and breadth of information available on computer systems is potentially unlimited. It is quite difficult for a court to be able to accurately determine, before making an order, the exact scope of information that should be disclosed. There is significant temptation to make the simplest order, allowing access to any information stored or otherwise available, in order to ensure that some relevant information is not missed. Certainly in preliminary

172 See, for example, A McCullagh and W Caelli, 'Extended case note and commentary: *Sony Music Entertainment (Australia) Limited & others v University of Tasmania & others* [2003] FCA 532' (September 2003) 53 *Computers & Law* 16 at 19, where the authors argue that both the investigatory software and the potential liability of individuals was misunderstood in *Sony v University of Tasmania*.

173 *Rank Film Distributors Ltd v Video Information Centre* [1982] AC 380; [1981] 2 All ER 76 at 78 per Lord Wilberforce.

174 (2004) 205 ALR 319; 59 IPR 299.

discovery this is not appropriate, because there has been little balancing of privacy interests with an assessed strength of the potential case. In *SmithKline Beecham plc v Alphapharm Pty Ltd*,¹⁷⁵ Finklestein J recognised that there is a limit to preliminary discovery, and that it is not a substitute for general discovery. His Honour stated that the object of preliminary discovery is ‘to disclose what is sufficient to permit the applicants to establish whether the elements of a cause of action are made out and to plead sufficient particulars to support a claim’.¹⁷⁶

Care must be taken when making an order for preliminary discovery to limit the scope appropriately. In cases concerning electronic records, at the very least this means recognising that (a) individual files stored electronically should be treated as individual documents; (b) wide access to ‘transitory data’ should not be encouraged; and (c) there may be many unrelated persons caught up in the discovery.

‘Documents’ — separating relevant electronic files

In *TLC v White*,¹⁷⁷ the Full Bench of the Queensland Court of Appeal held that although a computer server was a ‘repository of records’, it was still a ‘record’ for the purposes of the Fair Trading Act 1989 (Qld), and a ‘document’ for the purposes of the Acts Interpretation Act 1954 (Qld). The court approved of a decision by the applicant to enter into the respondent’s premises (under a warrant issued under the Fair Trading Act) and physically remove the respondent’s computer server, which contained the personal details of up to 20,000 individuals,¹⁷⁸ in order to investigate 39 complaints and the ‘generic practices which were indicated by the 39 complaints’.¹⁷⁹

There is generally no need for the entirety of a computer server to be considered a single record. It is usually simple for individual records stored on the server to be identified and removed. Further, even if a server is considered to be a ‘record’, wide disclosure in these types of cases does not appear to be justified, especially where there is no implication that the individuals whose privacy is to be injured have acted improperly. It would appear reasonable in these cases to impose a requirement that access to the server be limited to certain types of records or documents, or that copies of the server’s storage devices be made, allowing unnecessary personal information to be removed before access is allowed (in the case of Anton Piller orders), or allowing the

175 [2001] FCA 271 (unreported, Finklestein J, 19 March 2001, BC200101026).

176 *Ibid.*, at [26].

177 [2003] QCA 131 (unreported, de Jersey CJ, Davies JA and Atkinson J, 21 March 2003, BC200301227). Special leave was granted to appeal to the High Court, but the case was settled before the issues could be considered (see *TLC Consulting Pty Ltd v White* (unreported, HC, B14/2003, Gleeson CJ and Callinan J, 25 June 2003).

178 *TLC Consulting Services Pty Ltd v White* [2002] QSC 434 (unreported, Mullins J, 20 December 2002, BC200207856) at [11]:

the applicant’s business of an introduction agency is conducted Australia wide and has in the order of 20,000 current members. [The Applicant] deposes to the data on the server in relation to each client includes driver’s licence number, passport number, credit card details, key card details, telephone contact numbers, wage details, place of employment, education and qualifications, date of birth, nationality of member and parents, medicare number, names and ages of member’s children, names of members to whom the member has been introduced, email address and photographs.

179 *Ibid.*, at [37].

respondent to determine which record should be disclosed (in the case of discovery). This electronic procedure would be roughly equivalent to the physical practice of blacking out irrelevant information in hard copies of documents, or even more relevantly, handing over several files in a cabinet instead of the entire cabinet. Although this procedure may add extra overhead to the proceedings, it may be a necessary safeguard, particularly given the number of individuals likely to be affected.

Detailed analysis of information to be disclosed, as opposed to wholesale disclosure of all available data, could also prevent the problems associated with discovery of privileged documents. It has been suggested that the requirement that the persons executing a search on property ignore any document they can identify as being privileged¹⁸⁰ is not strong enough to protect the legal professional privilege¹⁸¹ or the privilege against self incrimination.¹⁸²

Restricting access to 'transitory data'

In *Universal v Sharman*,¹⁸³ the court appeared to waive the requirement that records are at risk of being destroyed for Anton Piller orders, if the information sought could be described as 'transitory data'. The logical extension of this principle leads to a situation where a party would be allowed to intercept ('preserve') all communications between users and service providers, in order to prevent the loss of the data that would otherwise occur. This is clearly not an appropriate action for private entities to be taking. It would not be so easy for a copyright holder to obtain similar information in the analogue world by, for example, obtaining an order that all phone conversations between a large entity and any individuals be recorded. A change in the medium used to communicate should not affect the legal protection of privacy of communications.

Considering unrelated persons caught up

Where discovery or other disclosure is granted, it should be limited to the information that is reasonably required on the evidence before the court. Information pertinent to two unrelated rights should not be disclosed merely on the basis that the respondent has access to both. In *Sony v University of Tasmania*, evidence that one user had possibly infringed Sony's copyright resulted in the disclosure of information relating to all users of a number of a university's servers. While it may be legitimate to disclose information that could show a conspiracy to infringe Sony's rights, this could have been done by disclosing only the information relevant to the user identified, which may have in turn identified any joint infringers. It does not seem necessary to disclose all of the university's information, which would mostly contain

180 See, for example, the order in *TLC Consulting Services Pty Ltd v White* [2003] QCA 131 (unreported, de Jersey CJ, Davies JA and Atkinson J, 21 March 2003, BC200301227) cl 6: 'If, in the course of examining the mirror copy of the hard drive of the server, the relevant officers of the appellant identify a document to which legal professional privilege could reasonably be considered to apply, those officers will not further examine the document'.

181 See B Fitzgerald, 'Is a server a record?' (2003) 10(4) *PLPR* 72.

182 *Rank Film Distributors Ltd v Video Information Centre* [1982] AC 380; [1981] 2 All ER 76.
183 (2004) 205 ALR 319; 59 IPR 299.

information about users wholly irrelevant to the proceedings, or possibly even users who had infringed Sony's copyrights but of which Sony had no previous knowledge, and would not have been able to satisfy the threshold for discovery. It is no answer to that threshold that one alleged infringement satisfies the requirements for any unknown and unrelated infringements. Showing prima facie evidence of a small number of infringements by one individual in a community can not justify an investigation into the affairs of all members of that community.

3.6 Defining the implied undertaking not to improperly use information

In all cases of discovery, there is an implied undertaking given to the court not to use the information disclosed for collateral or ulterior purposes, without leave of the court.¹⁸⁴ There is some suggestion that there is now 'a general rule that material provided or obtained by compulsory means during legal proceedings is prima facie subject to the implied undertaking'.¹⁸⁵

The undertaking prohibits use of information disclosed for a 'collateral or ulterior purpose'.¹⁸⁶ Strictly, this means that the information should not be used other than in the proceedings for which it was disclosed.¹⁸⁷ Groves considers that 'the weight of authority suggests that this requirement is interpreted narrowly',¹⁸⁸ and that the only two uses which will not be collateral or ulterior are to either use the material in the same proceeding, or to use the material in a proceeding for contempt against the party that disclosed the material.¹⁸⁹

In cases of preliminary third party discovery, however, the obvious problem is that the purpose of ordering discovery is often to identify the proper parties against which to proceed — it would seem counterintuitive to restrict use against those parties, once identified.¹⁹⁰ Instead, Kremer and Davies have suggested that the undertaking applies for the purpose that discovery was granted; in cases of identity discovery, the information disclosed can only be used to identify the 'person concerned', while in information discovery under the FCR, the information can only be used to make the decision whether or not to proceed with litigation.¹⁹¹

To avoid ambiguity, it is submitted that the best approach is to require that

¹⁸⁴ *Home Office v Harman* [1983] AC 280; [1982] 1 All ER 532.

¹⁸⁵ M Groves, 'The implied undertaking restricting the use of material obtained during legal proceedings' (2003) 23 *Aust Bar Rev* 314 at 320, citing *Cobra Gold Inc v Rata* [1996] FSR 819.

¹⁸⁶ *Alterskye v Scott* [1948] 1 All ER 469 at 470.

¹⁸⁷ *Riddick v Thames Board Mills Ltd* [1977] QB 881; [1977] 3 All ER 677.

¹⁸⁸ M Groves, 'The implied undertaking restricting the use of material obtained during legal proceedings' (2003) 23 *Aust Bar Rev* 314 at 325.

¹⁸⁹ *Ibid.*

¹⁹⁰ *Sony Corporation v Anand* (1981) FSR 398 at 401; approved of by Northrop J in *Autodesk Australia Pty Ltd v Dyason* (1994) 30 IPR 469 at 471. See also *Levi Strauss & Co v Barclays Trading Corp Inc* [1993] FSR 179; (1992) IP & T Digest 30, where Bromley J considered that Levi Straus was not bound by any implied undertaking not to use information revealed in preliminary discovery against others involved in a counterfeiting operation.

¹⁹¹ B Kremer and R Davies, 'Preliminary discovery in the Federal Court: Order 15A of the Federal Court Rules' (2004) 24 *Aust Bar Rev* 235 at 258.

leave of the court is always required before using information obtained on discovery against third parties. In appropriate cases, this leave could be granted at the time the order is made, for example to enable proceedings against identified parties to commence without delay where the applicants present a strong prima facie case at the preliminary discovery stage,¹⁹² or to allow the use of the results of an order tracing money to be used in the primary action.¹⁹³ However, where the case isn't as strong, or there will be many affected individuals, or the applicants propose to use the information for other purposes, for example to contact the identified persons even if they attract no liability,¹⁹⁴ an application to the court for leave could significantly reduce the risk of undue interference into the identified persons' privacy. The application would necessarily involve a quick review of the information disclosed, and enable the court to decide when it is appropriate for parties to act upon the information, at a time when the actual extent and contents of the information is known.

The requirement that the leave be obtained before information discovered is used or disclosed does not alleviate the concerns that information discovered may be overly broad. For example, if information private to a large number of individuals is disclosed, and leave is sought to bring an action against a small number of those individuals, the privacy of the rest of the group has still been infringed, in that their personal affairs have been rummaged through and a decision taken whether or not to proceed against them. It must be remembered that once private information about an individual has been disclosed, his or her privacy is already infringed — the requirement for leave is just a means of restricting aggravation of that injury.

3.7 Rolling orders against unknown defendants

In *Tony Blain v Jamison*,¹⁹⁵ Burchett J made an order analogous to an Anton Piller order, which allowed the plaintiffs to seize merchandise that infringed one of the plaintiff's trademarks from people who were unknown at the time the order was made. There was one defendant named as a representative of the class of defendants, and the order allowed seizure of merchandise from any person engaged 'in the business of selling or offering for sale to the public

192 See, for example, *Jade Engineering (Coventry) Ltd v Antiference Window Systems Ltd* (Ch Div (Patents Court), Jacob J, 25 January 1996, transcript by Marten Walsh Cherer):

When one is concerned with the protection of intellectual property rights, one often has a chain of different suppliers and the court has long held that a legitimate purpose can be their pursuit. So leave is given to use the information other than for the exact action before the court, to pursue others concerned with the infringement of the same right.

193 See, for example, *Omar v Omar* [1995] 3 All ER 571 at 577, where Jacob J considered that whether leave would be required depended upon whether the proposed use was within the 'broad purpose' of discovery. His Honour considered it safer, in order to remove doubt, that 'an order granting leave should be made, even if not strictly necessary'.

194 See *CHC Software Care Ltd v Hopkins & Wood* [1993] FSR 241, where it was held that it was legitimate for the applicant to contact the persons identified in the discovery process in order to 'put the record straight'. Cf *Roberts v Jump Knitwear* [1981] FSR 527 at 534, where Falconer J held that it was not permissible to use the names of customers of infringing material in order to put them on notice that the material supplied was infringing and hence 'complete the basis for a cause of action for infringement if they then went on to offer for sale or sell the garments in question'.

195 (1993) 41 FCR 414; 26 IPR 8.

merchandise'¹⁹⁶ that infringes the plaintiff's trademark. The order was limited to five concert venues and dates around Australia. The order differed to an Anton Piller order in that it did not require the defendants to allow entry onto their premises. However, in other respects the order is akin to an Anton Piller order, and Burchett J treated it as such, with reference to the English authorities. In *Tony Blain Pty Ltd v Splain*,¹⁹⁷ the New Zealand High Court went further, granting a prohibitory injunction and an order for delivery up and information discovery against any persons 'identified as persons who sell unlicensed merchandise at the relevant concert venues'.

The New Zealand case was heavily criticised by the Full Court of the Victorian Court of Appeal, partly on the basis 'it became binding upon a person only because that person was already in breach of it'.¹⁹⁸ However, Laddie J, in the High Court of England and Wales, referred to the New Zealand case with apparent approval and issued a similar order restraining unknown respondents from distributing the latest Harry Potter book.¹⁹⁹

These cases are an example of the increased scope of Anton Piller orders against unknown defendants. In Canada, this practice has been enlarged to allow 'rolling' orders, whereby an Anton Piller order is made against unnamed defendants and is valid for a one year renewable term.²⁰⁰ Such an order allows a plaintiff to seize documents and infringing merchandise from parties as it finds them. The information seized can be used, in turn, to identify further infringements and further defendants. Because the actions rarely go to trial, this method has become an effective way for Canadian intellectual property owners to penetrate what they regard as a shroud of secrecy surrounding infringers, and to efficiently enforce their rights by seizing infringing merchandise on penalty of contempt of court.

These rolling orders allow plaintiffs to effectively interrogate each link in a chain of infringement on penalty of contempt of court. They give plaintiffs a licence to seek out possible infringers and compel seizure of the goods and often disclosure of further information. They represent a strong interference with the rights of individuals to be let alone and be secure in their property, which may not be justified on the relatively low level of proof and judicial oversight that is required. The fact that the orders are much easier to comply with than to appeal against leaves the individuals affected in a difficult position, where an intellectual property owner is able to make extensive authoritarian demands on their privacy and property, as well as their knowledge about other persons. It is submitted that for these reasons it would not be appropriate for Australian jurisdictions to further develop orders against unknown defendants or to allow 'rolling' orders.

196 Ibid, at IPR 12.

197 [1993] 3 NZLR 185 (unreported, Anderson J, 25 March 1993).

198 *Maritime Union of Australia v Patrick Stevedores Operations Pty Ltd* [1998] 4 VR 143 at 161.

199 *Bloomsbury Publishing Plc v Newsgroup Newspapers Ltd* [2003] EWHC 1087 (Ch) (unreported, Laddie J, 7 May 2003, Transcript: Smith Bernal).

200 See, generally, J Berryman, 'Recent Developments in Anton Piller Orders: John and Jane Doe, rolling along in Canada', *Oxford Intellectual Property Research Centre Working Paper Series*, No 4, November 2001 <<http://www.oiprc.ox.ac.uk/EJWP0401.html>> (accessed 14 July 2004).

3.8 Safeguards in ex parte applications

Ex parte orders for discovery and delivery up should only be granted in situations where there is an immediate threat that information will be destroyed or irreparable damage suffered.²⁰¹ Unfortunately, there is always a risk that the applicant's fears of damage are exaggerated or polarised, and without the presence of the respondent, it is difficult for the court to objectively determine the risk of potential damage.

Of even greater risk is the suggestion that the threat of destruction can be implied. We have already seen that the threat of destruction was satisfied in *Universal v Sharman*²⁰² by recognition that the data was 'transitory'. In *Sky Channel v Yahmoc Pty Ltd*,²⁰³ Allsop J granted an Anton Piller order after recognising that there was 'no particular indication that the [respondents] will act in any way improperly',²⁰⁴ but implying the risk of destruction on the basis that the respondents had prima facie knowingly infringed the applicants' rights and that the offending device (a smartcard which allows decryption of a broadcast television signal) was small and easy to remove and hide.

The principle expressed in this case is somewhat disingenuous. It effectively nullifies the long established requirement that an Anton Piller order only be granted where there was an immediate risk that the respondent would destroy the evidence if he or she were given notice, in the sense that it can be satisfied by showing a prima facie case that the respondents knowingly infringed the applicant's rights. This case is an example of the dangers inherent in ex parte applications, where the court is liable to make concessions or changes to procedure at the behest of counsel without the beneficial counterargument from opposed counsel.

Duty of candour

It is a well recognised principle that applicants in ex parte proceedings have a heavy duty of candour owed to the court.²⁰⁵ In practice, however, this duty of candour can not always protect the court from being misled, even without fault of the applicant. In ex parte applications, the applicant can not be in

201 In *Sega Enterprises Ltd v Alca Electronics* (1982) FSR 516 at 525 per Templeman LJ observed that the power to make orders for discovery:

should not be exercised in interlocutory proceedings, and certainly not ex parte, unless the court is reasonably satisfied that the plaintiff will, or probably will suffer irreparable damage if there is any delay in ordering discovery. Where the court is satisfied — and on ex parte applications, the court cannot be certain; it must act on the evidence which is before it — that the plaintiff will or may probably suffer irreparable damage, then the court may act with all the speed with which the court is capable and may impose ex parte orders for discovery. But such orders should never be made as a matter of course — never merely as part and parcel of an Anton Piller order — without investigation of the circumstances of each case and without the court coming to the conclusion that it is necessary for the long-term protection of the plaintiff that such a Draconian course should be taken.

202 (2004) 205 ALR 319; 59 IPR 299.

203 (2003) 58 IPR 63.

204 *Ibid*, at [7].

205 *Liberty Financial Pty Ltd v Scott* [2002] FCA 345 (unreported, Weinberg J, 26 March 2002, BC200201174) at [73]; *Garrard v Email Furniture Pty Ltd* (1993) 32 NSWLR 662 at 676; *Thomas A Edison Ltd v Bullock* (1912) 15 CLR 679.

possession of all relevant facts, indeed the applicant is usually making the application because they do not have all the relevant information. While the importance of the duty of candour is certainly not to be diminished, it can not consistently be relied upon to provide a guarantee that a given order is justifiable with regard to all the circumstances. This is the main reason that invasive ex parte orders should not be lightly granted, and it must be kept in mind in all applications.²⁰⁶

Amicus curiae

In some jurisdictions, when dealing with ex parte applications, the court may seek amicus curiae to present the case of the unrepresented party. This procedure was considered ‘invaluable’ by Lord Denning MR when dealing with a particularly important principle in an early ex parte Anton Piller decision.²⁰⁷ In *Tony Blain v Splain*,²⁰⁸ Anderson J in the New Zealand High Court considered that it would be helpful where the court was asked to grant an Anton Piller against unknown persons to appoint an amicus curiae to represent those unknown persons, on the basis that ‘there is always a diffidence about extending the court’s activities to persons by way of civil search warrants and interrogatories’.²⁰⁹ This approach was recently approved of by Laddie J, in the High Court of England and Wales in *Bloomsbury Publishing Plc v Newsgroup Newspapers Limited*,²¹⁰ but in both cases the application and potential damage was considered too imminent to warrant the delay that the process would cause.

Most recently, this practice was used in the Canadian Federal Court in *BMG v John Doe*,²¹¹ where members of the recording industry sought discovery from five ISPs against alleged users of the Kazaa and iMesh filesharing networks. Even though the application was not made ex parte, the court granted intervenor status to two public interest groups, implicitly recognising that the best interests of unknown individuals are not always adequately represented by the parties who hold the keys to their identity.

It is submitted that when an order is sought against an intermediary that would disclose the activities of individuals, the court should consider appointing amicus or amica curiae to prevent the injustice that is likely to occur when such an invasive order is granted without representation. This procedure would go some way to prevent the twin risks that either there can be no respondent party, in ex parte applications, or that the respondent party merely consents to the applicant’s request, without considering the rights or expectation of the affected individuals.

3.9 Costs

Where applicants seek discovery of information from intermediaries, the question of costs will be very relevant to the process. Not only is it generally unfair for a third party to be put to significant expenditure in order to provide

²⁰⁶ *Sega Enterprises Ltd v Alca Electronics* (1982) FSR 516 at 525 per Templeman LJ.

²⁰⁷ *Ex parte Island Records Ltd* [1978] Ch 122; [1978] 3 All ER 824.

²⁰⁸ [1993] 3 NZLR 185.

²⁰⁹ *Ibid.*, at 188.

²¹⁰ [2003] EWHC 1087 (Ch), (unreported, Laddie J, 7 May 2003, Transcript: Smith Bernal).

²¹¹ [2004] FC 488 (Can Fed Ct, Von Finckenstein J, 31 March 2004).

information about other persons, but the threat of costs in objecting to the disclosure may prevent it from properly doing so. As the third parties are generally the only parties who have standing to challenge a preliminary order for discovery, they must not be discouraged from effectively representing the rights of their users.

In *C7 Pty Ltd v Foxtel Management Pty Ltd*, where Gyles J, when considering a large scale application under FCR O 15A r 6, said:

It needs to be borne in mind that this is an extraordinary jurisdiction. It provides for compulsory access to the private affairs of members of the community in order that somebody else can determine if they have a case against that party and the threshold set by O 15A r 6(a) is not very high. There is much to be said for the view that a respondent in these circumstances is entitled to put the applicant to proof except in a clear case. Some judges have been disposed to make orders which, to a greater or lesser extent, leave costs to be determined after the result of preliminary discovery and inspection is known, and even to depend upon, to some extent, the fate of the litigation which ensues. I am not persuaded of the merit of that approach. An application pursuant to O 15A is a discrete application and may never lead anywhere. There is no reason why a party which is out of pocket because of costs should await some indefinite future event.²¹²

Similarly, where a reasonable question arises after discovery has been ordered about the interpretation or compliance with the order, the respondent will ideally not be liable for the cost of hearing that question.²¹³

It is suggested that in all but the most trivial of cases where third party discovery is sought against an intermediary, costs should be borne by the applicant for the application and execution of orders, including any non-frivolous objections as to the scope and propriety of the orders. Where it is reasonable for the costs to be made as part of a later process against persons identified by the discovery, it would seem reasonable to follow the approach of Finklestein J in *SmithKline Beecham plc v Alphapharm Pty Ltd*²¹⁴ and Burchett J in *Cappuccio v Australia & New Zealand Banking Group Ltd*,²¹⁵ where the costs of discovery were made subject to a later proceeding, if instituted before a certain date, and to be borne by the applicant otherwise.

3.10 Conclusion

The tensions between online privacy and intellectual property enforcement are widespread, varied and largely unresolved. The practice of using litigation against unrelated intermediaries with a view to obtaining private information about individuals is now firmly entrenched, and the justifications for doing so, while not universal, are often important. While it is obviously important for parties to be able to enforce their rights, courts must recognise that it is equally important for individuals to be safe in their privacy. This recognition must in turn force the further development of judicial safeguards when courts exercise

212 [2001] FCA 1864 (unreported, Gyles J, 21 December 2001, BC200108239) at [50].

213 Cf *Sony Music Entertainment (Australia) Ltd v University of Tasmania* [2003] FCA 805 (unreported, Tamberlin J, 29 July 2002), where Tamberlin J granted Sony's costs where the universities questioned whether the discovery provided should include backup copies that had been overwritten.

214 [2001] FCA 271 (unreported, Finklestein J, 19 March 2001, BC200101026).

215 [1999] FCA 1188 (unreported, Burchett J, 23 August 1999, BC9905808).

the discretion to grant preliminary discovery, prompting a more thorough balancing of the competing interests involved. The suggestions outlined above are neither comprehensive nor conclusive; the most important concept is that the privacy interests of all parties affected by litigation needs to be recognised, not just those of the represented parties.

The ultimate aim of this article is not to advocate a position where it becomes impossible for intellectual property owners to enforce their rights, but to promote discussion of the appropriate balance between privacy and intellectual property enforcement. The rights of intellectual property holders and the rights of individuals to privacy are not necessarily mutually exclusive — it is possible to develop preliminary discovery in such a manner that relevant information can be sought without infringing the rights of innocents. The struggle between intellectual property owners and individuals for control of the rights to use and the rights to shape technology is a complex one, and only recognition and understanding of the key issues can help to restore the delicate balance.