

12-1-2002

## Building client confidence in ODR: how effective is the new privacy legislation for cyberspace?

Lisa Goldacre

---

### Recommended Citation

Goldacre, Lisa (2002) "Building client confidence in ODR: how effective is the new privacy legislation for cyberspace?," *ADR Bulletin*: Vol. 5: No. 7, Article 3.  
Available at: <http://epublications.bond.edu.au/adr/vol5/iss7/3>

This Article is brought to you by [ePublications@bond](mailto:ePublications@bond). It has been accepted for inclusion in ADR Bulletin by an authorized administrator of [ePublications@bond](mailto:ePublications@bond). For more information, please contact [Bond University's Repository Coordinator](#).



Privacy law and ADR

# Building client confidence in ODR: how effective is the new privacy legislation for cyberspace?

Lisa Goldacre

The growth in electronic commerce and online transactions has seen a corresponding growth in the use of information technology for dispute resolution. The most obvious form of ADR for the virtual community is online dispute resolution (ODR). ODR services are not limited to disputes that arise in cyberspace but can be, and indeed are, used for disputes that arise in the real world.

ODR is described by the National Alternative Dispute Resolution Advisory Council (NADRAC) as 'processes that are delivered substantially or entirely through online communications'.<sup>1</sup> The structure for provision of ODR services can take three main forms. One is by independent practice, whether as part of an existing ADR business or a stand alone service dedicated to the resolution of disputes in an online forum; the second is as part of the service offered by a business operating online; and the third is as part of a trustmark scheme.<sup>2</sup>

It has been said that 'ODR schemes will only work if underpinned by technological-organisational mechanisms promoting certainty and trust'.<sup>3</sup> The protection of clients' privacy can be seen as central to the promotion of certainty and trust for two reasons.

First, that greater protection of clients' privacy will increase confidence, and therefore use of online services.<sup>4</sup> As with all areas of business in e-commerce, gaining consumer trust and confidence has been seen as one of the factors crucial to continued growth and success.

Anxiety surrounds the many ways that technology can collect information that people may consider to be private, including the use of devices such as cookies<sup>5</sup> and web bugs.<sup>6</sup> Further, this may occur when people are unaware that information is being collected and do not know to what use it will be put. Some

other risks in relation to interferences with privacy have been identified by the Federal Privacy Commissioner and include concerns about 'identity creep' and data mining.<sup>7</sup> What is not certain is how much invasion of people's privacy is occurring online. According to surveys of consumers and business commissioned by the Office of the Federal Privacy Commissioner:

Eighty-four per cent [of people responding to the consumer surveys] believed that businesses often transfer or sell customer details in mailing lists to other businesses. Yet 87 per cent of all respondents said they would be 'concerned' or 'very concerned' if a retailer passed on name, age, address and interest details to another retailer without their knowledge ... however ... [90] per cent of organisations responding to the business survey said they never sold, rented out or transferred customer details to other organisations. Fourteen per cent said they regularly obtained information about customers or potential customers from other organisations.<sup>8</sup>

As is apparent, and was to the Federal Commissioner, there may be some disparity in what is actually occurring, at least to the extent of invasions of privacy and misuse of information, and what consumers believe to be happening. Perceptions regarding lack of privacy protection in the online environment can be just as much a hindrance to the growth of ODR as can the actuality. It is these concerns that need to be met in order to build consumer confidence in ODR.

Second, protection of 'private' information disclosed in an ODR process is consistent with ADR theory. Adequate protection of confidential information is fundamental to many ADR processes, be they online or otherwise.<sup>9</sup> While not every ADR process has confidentiality at

its core, often assurances that what is exchanged remains confidential, even if in a limited way, are paramount.<sup>10</sup> For example, confidentiality in a family mediation may have a different meaning from that of a commercial dispute dealing with commercially sensitive information. It is often understood implicitly or expressly that what is disclosed in the course of a family mediation may be discussed with new partners or significant others, such as parents.

Confidentiality in ADR is readily apparent when we think about the physical world. Consider how we walk into a room, close the door and make explicit the need for confidentiality. In a virtual world, the doors are less obvious, but may be needed just the same.

Given the fact, therefore, that the protection of clients' privacy is important for increasing user confidence in ODR processes, this article examines the effectiveness of the recent amendments to the *Privacy Act 1988* (Cth) (the Act) in building that confidence.

## How is privacy protected in ODR processes?

Mechanisms which can enhance the protection of people's privacy online include technology, the law and voluntary standards.

### Technology

Protecting privacy through the use of technical devices includes employing systems that result in increased security, such as encryption, public key infrastructure (PKI), firewalls and the like.<sup>11</sup>

### The law

There are a number of actions at common law, such as an action for breach of confidence, the remedies for which may provide protection of parties' confidential information.<sup>12</sup>

As far as legislation is concerned, a number of Acts specifically seek to regulate activity on the internet.<sup>13</sup> The most significant attempt to ensure individuals' privacy and protection from unauthorised interferences with personal information is the *Privacy Amendment (Private Sector) Act 2000* (Cth). These amendments to the *Privacy Act 1988* (Cth), which came into force in December 2001, have changed how the private sector collects, stores, uses, secures and transfers information. There are detailed

procedures that must be complied with in relation to all of the above. Should an individual request it, private sector organisations must now give access to any information held about them and, if asked, make corrections. These requirements are known as the National Privacy Principles (NPPs).<sup>14</sup>

The main objective of the amendments is to provide individuals with greater protection against unauthorised interferences with their personal information. They seek to confer 'information privacy' rights rather than 'a right to privacy' as such.<sup>15</sup>

The Government has embarked on a co-operative model of regulation: self-regulation against the background of legislative minimum standards.<sup>16</sup> Businesses that are required to comply with the Act can opt out of the legislation provided there is an approved privacy code in place.<sup>17</sup> Similarly, if an exempt business wanted to 'opt-in', the legislation makes provision for that to occur.<sup>18</sup>

In its discussion paper on 'Dispute resolution in electronic commerce', the Consumer Affairs Division of the Federal Treasury asserts that 'the amendments to the *Privacy Act* will give consumers greater assurance in relation to the security of information online'.<sup>19</sup>

Therefore, the question to be asked is whether the amendments to the Act are an effective mechanism for protecting personal information in the context of ODR.

## What information is covered by the Act?

Privacy is not defined anywhere in the Act. Instead, particular types of information are protected by the NPPs. Information that is protected from an interference with privacy is that which can be classified as 'personal information'. The Act largely applies to the collection of personal information for inclusion in a record or generally available publication.<sup>20</sup>

Personal information means any information or opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent or can reasonably be ascertained from that information or opinion.<sup>21</sup>

Generally, an ODR provider would have information of this kind in relation

to a user of their service. It is suggested by one commentator that, even if the information itself cannot be information from which an individual's identity is apparent or can reasonably be ascertained, it is a question of fact whether the given circumstances may lead to that identity becoming known.<sup>22</sup> This is an important consideration for providers of online services, which may hold a range of information about visitors to their web sites who make initial inquiries but do not necessarily become clients.

For example, an ODR provider may have email addresses, click-trails or certain information from cookies which at first glance may not be information that would fall readily into the category of 'personal information', but when combined in certain circumstances may be information from which an individual may be identified. As mentioned earlier, internet users' concerns appear to extend to this unknown collection and storage of seemingly innocuous information which may be later compiled into valuable information. The definition of personal information does not assist with this issue.

'Sensitive information' is a subset of personal information. It is defined as information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health information about an individual.<sup>23</sup>

Clearly, an ODR provider in the course of resolving a dispute may collect this type of information.

The Act is concerned with protecting individuals' privacy. An individual is defined to mean a natural person.<sup>24</sup> Therefore, a corporation cannot avail itself of the protections available under the Act. One difficulty that might arise in the context of ODR is that the Act is predicated on the view that information disclosed or collected about an individual belongs only to that individual and that no one else has a protectable interest in that information being disclosed or collected. This may not always be the case in relation to many disputes. In a family dispute, for example, more than one family member may have reasons not to have some sensitive information about



another family member disclosed or even collected.

### Who is covered by the Act?

Until the recent amendments to the Act, the legislation was concerned only with Commonwealth agencies and certain private sector entities including, for example, credit providers. The amendments have the effect of extending the operation of the Act to the private sector in general, subject to some exemptions.

Pursuant to Pt III Div 1 of the Act, an organisation will interfere with the privacy of an individual, and so offend the provisions of the Act, if any act or practice of the organisation breaches an NPP or an approved privacy code.<sup>25</sup> An organisation includes an individual, body corporate, partnership, an unincorporated association or a trust.<sup>26</sup>

If an organisation is a small business as defined by the Act, it will be exempt from having to comply with the NPPs.<sup>27</sup> However, a small business may still be required to comply if they:

- have an annual turnover of \$3 million or more;
- provide a health service;<sup>28</sup> or
- are a contracted service provider for the Commonwealth.

It does not seem likely that many ODR providers at this stage would have a turnover of more than \$3 million, unless related to another body corporate; however, they may have a contract with the Commonwealth to provide those services. It is not likely that an ODR provider whose services were limited to the provision of dispute resolution only would fall within the definition of a health service.<sup>29</sup>

Further, s 6D(4)(c) and (d) of the Act states that an organisation will not be a small business operator and therefore exempt from the requirements of the Act, if they disclose or collect personal information about another individual, to or from anyone else, for a benefit, service or advantage. Small business status will not be denied in this situation if the ODR provider has the consent of the other individual or is required or authorised to do so under legislation.<sup>30</sup>

These sections are not described any further in the Act. The Explanatory Memorandum provides no further indication regarding how these sections are to be read or the purpose behind their

inclusion. In one of its publications on the application of the Act, the Office of the Federal Privacy Commissioner summarises these sections as referring to organisations with a turnover of \$3 million or less 'that trade in personal information'.<sup>31</sup> Therefore, are these provisions intended to extend to services for which their primary activity is to resolve disputes?

On the face of it, it is easy to imagine a situation where an ODR provider may collect personal information about another and in limited circumstances disclose this information in the course of an ADR process, for a benefit, service or advantage. If these provisions were to be read as not limited to organisations with a turnover of \$3 million or less 'that trade in personal information', many ODR providers would no longer be considered an exempt small business operator unless they had specifically obtained the consent of the individual or were required to collect or disclose the information under law. Non-exempt small businesses have until December 2002 to comply with the Act.

As noted by Professor Greenleaf, one of the difficulties in ascertaining exactly what is covered by the legislation is the dearth of judicial interpretation of the provisions of the Act, resulting in the need to rely largely on the Federal Privacy Commissioner's interpretation of the Act in the form of that Office's guidelines.<sup>32</sup>

One example is the Office's response to an FAQ regarding the collection of sensitive information by an ADR provider about third parties pursuant to s 10 of the Act.<sup>33</sup> It is unclear what they have based their answer on. They indicated that an ADR scheme could collect sensitive information about a third party without consent. The difficulty with the answer given by the Office of the Federal Privacy Commissioner is that presumably the answer relies on the fact that the collection is required by law. It would be one of the parties to the dispute, however, which required the sensitive information as necessary for the establishment, exercise or defence of a legal or equitable claim. It is not the ADR provider's claim that is in question.

Further, not all ODR processes are the same. It may be in arbitration or under legislative provisions requiring parties to participate in an ADR/ODR process that this answer would be accurate. Not all

processes are advisory in their nature, such that would require the collection by the impartial person of information from a third party to be necessary for the establishment, exercise or defence of a legal or equitable claim. It would seem that in these circumstances the ODR provider would need to obtain consent from the third party to collect the information, so as not to breach the NPPs, and also consent from the party or parties to the dispute so as to avoid potential breaches of any obligation of confidence that are owed at common law.

### Remedies available under the Act

Pursuant to Pt V of the Act, the Privacy Commissioner is required to investigate complaints of interferences with privacy of an individual. Part V also outlines the Commissioner's powers of investigation.<sup>34</sup> Businesses that are within an approved industry code have their own mechanisms for dealing with complaints. The Commissioner can review a code adjudicator's determination.<sup>35</sup>

If the Commissioner finds a complaint substantiated pursuant to s 52 of the Act, the Commissioner may make a determination. The determination can include a declaration that the offending conduct is not to be repeated or continued, that the respondent should perform 'any reasonable act or course of conduct to redress any loss or damage suffered, which can include a 'specified amount by way of compensation'.<sup>36</sup> However, any determination made by the Commissioner would need to be enforced by commencement of proceedings in the Federal Court or Federal Magistrates Court.<sup>37</sup> In addition to s 52, 'the Commissioner or any other person' may apply to the Federal Court for an injunction to restrain a person who has engaged, is engaging or proposing to engage in conduct that would be in contravention of the Act.<sup>38</sup>

### Enforcement

It appears that individuals who deal with 'organisations' within Australia now have some increased protection in relation to personal information as defined by the Act.<sup>39</sup> The Act also provides protection in relation to the transfer of personal information outside Australia.<sup>40</sup>

In the context of ODR, however, where many of the providers of such a service are located overseas, the issue is whether these operators have to comply with the Act if someone in Australia uses their service. If the goal is to promote client confidence in ODR so that there is trust and certainty that personal information is not subject to unauthorised interferences with privacy, then the Act needs to apply equally to services accessed in Australia, irrespective of where an ODR provider's server is located.

If a person wishes to commence proceedings against another for a breach of the Act and the other party is located overseas, the immediate question is: can they bring the matter before the Federal Court for determination?

There is a complex body of rules used to determine whether an Australian court would, first, have jurisdiction to hear such a matter (law of forum) and, second, if it did, which law should be applied to determine the rights of the parties (choice of law).<sup>41</sup> Historically, the law has been able to accommodate changes in technology. Courts have developed rules to suit new forms of technology, and indeed issues such as the law of forum and choice of law have been addressed in relation to telephones and faxes.<sup>42</sup>

In relation to the issue of whether or not Australian courts have jurisdiction to hear matters that have arisen as a result of online activities where the business's server is located overseas but the relevant access occurs in Australia, this has been dealt with in a number of cases recently.<sup>43</sup> While the law in this area is still developing and at times is problematic, the principle which is slowly emerging is that if you are conducting business or providing a service that is accessed in Australia, the overseas provider will need to comply with the local laws.<sup>44</sup> This would include, therefore, the requirements under the Act.

The next step is then to determine whether any order made by the Federal Court pursuant to the Act can be enforced. The difficulty of enforcing any order made by an Australian court<sup>45</sup> against a foreign defendant undermines the effectiveness of the Act. There is no ready solution to this. Countries often have in place legislation that allows them to recognise and enforce judgments of another jurisdiction, but there are usually limitations to using these Acts.<sup>46</sup>

A number of co-operative international initiatives exist that seek to overcome this problem.<sup>47</sup> One example is the *Hague Convention*<sup>48</sup> which seeks to alleviate these problems by providing a clear set of consistent rules to be followed in all jurisdictions.<sup>49</sup> There is of course the practical problem of the high cost of seeking enforcement of an order in a foreign jurisdiction for what may be a low cost transaction.

In an internet context, even if the organisation in breach of the provisions of the Act were in Australia, the very nature of the internet raises its own problems in relation to enforcement of orders. When a provision of a statute is contravened and a judgment given to that effect, it is important that the remedy granted be enforceable. In an internet context, one remedy sought might be an injunction restraining certain representations from being made on a website, as was the case in *ACCC v Purple Harmony Plates Pty Ltd*.<sup>50</sup>

Here the respondents ignored the court order prohibiting the making of misleading and deceptive claims about their products in contravention of s 52 of the *Trade Practices Act 1974* (Cth). They continued with their offending conduct via another website and by links to other sites. They also failed to comply with the corrective advertising orders made against them, such as the requirement to have a 'pop-up' notice on the website specifically outlining the orders of the Federal Court and that refunds were available to consumers. In later proceedings they were found to be in contempt of court and fined. The ACCC's application to have the websites deregistered was refused. As was shown in this case, and a number of other cases before the Federal Court,<sup>51</sup> enforcement of orders of this nature is difficult where the internet has been used, due to the ephemeral nature of the internet itself. Businesses are very mobile and can just move on to a new website and start again. The authority of the court issuing the order is also at risk if rogue operators can ignore court orders, shut down and move on to another URL. These difficulties were alluded to in *Macquarie Bank v Berg*<sup>52</sup> as was the reason why orders were declined (equitable remedy of injunction).<sup>53</sup>

Therefore, the same problems that have appeared before the Federal Court in relation to enforcement of like orders

under the *Trade Practices Act* would undoubtedly occur in respect of orders made restraining a contravention of the Act. The lack of effective enforcement of court orders also undermines the confidence of users of internet services. It is problematic that there is no 'sovereign' in cyberspace.<sup>54</sup>

It is somewhat paradoxical that the problems associated with the enforcement of the law in cyberspace might be a sticking point for some ODR providers endeavouring to use a piece of legislation in the hope of engendering client trust and confidence, when one of the reasons for the emergence of ODR has been difficulties of access to the law and remedies, particularly in B2C (business to customer) transactions.

It would seem, therefore, that the Treasury's assertion that 'the amendments to the Act will give consumers greater assurance in relation to the security of information online' is overstated and optimistic if it is relied upon solely as a legal mechanism for protecting people's personal information.<sup>55</sup> The Act will not apply to all ODR providers or in all instances where personal information is gathered or used. Further, the 'borderless' nature of the internet limits the effectiveness of the Act.

### **Voluntary standards as a self-regulating mechanism**

The most likely way for the Act to provide an effective mechanism for building client confidence in ODR is through the adoption of the NPPs as voluntary standards in conjunction with the legislation.

The adoption of the Act's NPPs as a voluntary standard to aid self-regulation of ODR, and indeed ADR generally, is consistent with NADRAC's report to the Federal Attorney-General on standards for ADR and its recent paper suggesting principles for good practice in relation to dispute resolution and information technology.<sup>56</sup> A number of organisations and commentators have suggested best practices models for ODR services and specifically for B2C dispute resolution.<sup>57</sup>

One common criterion in the best practice models or benchmarks is described as 'accessibility'.<sup>58</sup> This means not just that the service be accessible, convenient and as easy to use as possible, but also in the sense of being transparent — that all relevant information needed to



make an informed decision about whether to use the ODR service or not is accessible. This would include information about an ODR service provider's policy in relation to the collection, storage and use of clients' personal information.

As mentioned earlier, obligations of confidence are integral to ADR practice. An ODR provider will often already be subject to such a duty, either at common law or pursuant to other legislation.<sup>59</sup> Therefore, would adopting the requirements of the Act be any more onerous than what an ODR provider may already be required to do now? The answer is probably 'yes'. The NPPs refer not just to disclosure of personal information, but also to the collection of personal information of another person, how it is stored, secured and transferred. It also gives individuals a right of access. It is, therefore, wider in its scope than the duty to keep certain information confidential.

A matter that should be considered by an ODR provider before adopting the NPPs is that opting into the privacy scheme and placing a statement to that effect on a website means that the policies outlined in that statement must be adhered to. An ODR provider who failed to adhere to its own privacy statement could run the risk of being sued under the *Trade Practices Act* for a contravention of s 52, in a similar fashion to Toysmart.com in the US.

Late last year Toysmart.com, a company largely owned by Walt Disney, tried to raise money by selling their records and databases. This included information about children.

Toysmart.com was accused of violating its internet privacy policy in the way it used its cookies (to create a database with addresses and so on). No formal charges were filed by the New Jersey division of the Federal Trade Commission (FTC) consumer affairs (an action would have been brought by the FTC under the equivalent of s 52 of the *Trade Practices Act*). The matter was settled with Toysmart.com paying \$50,000 and agreeing to post a link to its privacy policy on the front doors of its e-commerce sites.<sup>60</sup>

### Conclusion

Gaining consumer trust and confidence is essential for the continued

growth of ODR. A key element in this is ensuring that personal information disclosed in an online setting is protected from unauthorised access and use. The *Privacy Act* regulates the use, access, collection, storage and disclosure of some types of information by some types of private sector organisations. However, the coverage and scope of the Act is limited in an ODR context because of the breadth of the small business exemption and the fact that the majority of ODR providers are located outside Australia. The Act cannot overcome the problems that are generic to all e-commerce businesses. As can be seen from the above discussion, the global nature of the internet raises complex jurisdictional issues which can impact on the level of privacy accorded to an individual. Further, it is still unclear how the Government will be able to enforce effectively its legislation in respect of offshore providers of ODR.

Yet ODR providers need to consider the benefits of opting into the new privacy legislation regime. As there often is already an existing duty of confidentiality imposed on mediators, and due regard for confidentiality in ADR processes is encompassed in the standards for ADR providers as outlined by NADRAC, voluntary compliance with the NPPs as set out in the Act should be considered 'best practice'. The effectiveness of the Act as a mechanism for building client confidence in ODR is cumulative — it will work best if it is both used as a legal mechanism and the NPPs are adopted as voluntary standards by ODR providers. ●

*Lisa Goldacre is an Associate Lecturer at the Law School, University of Western Australia. She can be contacted at [lgoldacr@ecel.uwa.edu.au](mailto:lgoldacr@ecel.uwa.edu.au).*

*The author would like to thank Robyn Carroll for her insightful comments, excellent supervision and enduring patience. All errors and omissions remain the author's responsibility. This paper was presented at the 6th National Mediation Conference, September 2002, Canberra.*

### Endnotes

1. NADRAC submission *ADR in E-Commerce* in response to the

discussion paper released by Consumer Affairs Division of the Federal Treasury October 2001 at p 2 available at [www.nadrac.gov.au/aghome/advisory/nadrac/ecommerce/EcommerceADRsub2.doc](http://www.nadrac.gov.au/aghome/advisory/nadrac/ecommerce/EcommerceADRsub2.doc).

2. Hörnle J 'Disputes solved in cyberspace and the Rule of Law' 2001 (2) *The Journal of Information, Law and Technology* <[elj.warwick.ac.uk/jilt/01-2/hornle.html](http://elj.warwick.ac.uk/jilt/01-2/hornle.html)> at Section 2, in turn referring to Consumers International *Disputes in Cyberspace* 2000 at pp 11-12 and Wilkens M, Vahrenwald A and Morris P *Out-of-Court Settlement Systems for E-Commerce: Report of an Exploratory Study* European Union Joint Research Centre (2000) at p 11, available at <[dsa-isis.jrc.it/ADR/Reportv20apr.pdf](http://dsa-isis.jrc.it/ADR/Reportv20apr.pdf)>. To Hörnle's third category the author would include independent schemes and providers of traditional ADR services who might add an ODR system to their existing practice.

3. Bygrave L 'Online dispute resolution — what it means for consumers' Domain Name Systems and Internet Governance Conference, Baker & McKenzie Cyberspace Law and Policy Centre in conjunction with the continuing Legal Education Programme, University of NSW 7 May 2002 at p 8 available at <[www.bakercyberlawcentre.org/2002/Domain/Bygrave\\_ODR.pdf](http://www.bakercyberlawcentre.org/2002/Domain/Bygrave_ODR.pdf)>. Dr Bygrave is of the view that the term 'electronic dispute resolution' (EDR) would be more appropriate and possibly less misleading as it would encompass more accurately those processes that take advantage of technology but are not immediately available online. Similar concerns about security, confidentiality and privacy are identified in the NADRAC background paper *Online ADR* January 2001 available at <[www.nadrac.gov.au/aghome/advisory/nadrac/ADR.html](http://www.nadrac.gov.au/aghome/advisory/nadrac/ADR.html)>. On the issue of whether the *Privacy Act* is able to engender trust in cyberspace, see also Clarke R 'Privacy as a means of engendering trust in cyberspace commerce' (2001) 24(1) UNSW Law Journal 290.

4. See, for example, the discussion paper 'Dispute resolution in electronic commerce' Consumer Affairs Division Department of Treasury available at <[www.ecommerce.treasury.gov.au/publications/DisputeResolutioninElectronicCommerceDiscussionPaper/index](http://www.ecommerce.treasury.gov.au/publications/DisputeResolutioninElectronicCommerceDiscussionPaper/index)>.

htm>.

5. See Lim Y F *Cyberspace Law: Commentries and Materials* Oxford University Press Melbourne 2002 pp 114–15.

6. Above note 5 at pp 118–19.

7. Crompton M 'What is privacy?' Privacy and Security in the Information Age Conference Melbourne 16–17 August 2001 p 5 available at <[www.privacy.gov.au](http://www.privacy.gov.au)>.

8. Above note 7 at pp 3–4.

9. For example, see Astor H and Chinkin C *Dispute Resolution in Australia* LexisNexis Butterworths Sydney 2002 pp 178–87.

10. Above note 9.

11. For a further discussion of these issues see McCullagh A and Commins I 'Cryptography: from information to intelligent garbage with ease' in Fitzgerald et al *Going Digital 2000: Legal Issues for E-Commerce, Software and the Internet* (2nd ed) LexisNexis Butterworths Sydney 2000 p 207.

12. See further Muirhead S 'A risk management approach to legal liability in the ADR process' (2002) 13 ADRJ 148 at pp 151–52; and Carroll R 'Mediator immunity in Australia' (2001) 23 *Sydney Law Review* 185 in relation to mediators' immunity.

13. *Telecommunications Act 1997* (Cth) regarding privacy obligations for ISPs; the *Telecommunications (Interception) Act 1979* (Cth). See generally Gunning P 'Legal aspects of privacy and the internet' in Fitzgerald et al above note 11 p 217.

14. Schedule 3 of the Act.

15. Whether an independent cause of action lies for a breach of the tort of invasion of privacy in Australia was the subject of judicial consideration in the recent High Court case of *ABC v Lenah Game Meats Pty Ltd* (2001) 76 ALJR 1.

16. Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth).

17. Section 16A of the Act.

18. Section 6EA of the Act.

19. Above note 4 at pp 7–8.

20. Section 16B of the Act. For a discussion of the meaning of this section see Greenleaf G 'Key concepts undermining the NPPs — a second opinion' (2001) PLPR 8(1) 1 in response to Gunning P 'Central features of Australia's private sector privacy law' (2001) PLPR 7(10) 189. Other

difficulties or 'gaps' that appear in the NPPs include:

- direct marketing exception in NPP 2.1(c); and
  - personal information that is collected for research — the only exemption regarding research is limited to health information by NPP 2.1(d). This may be important for ODR and the provision of transcripts and much needed empirical data.
21. Section 6 of the Act.  
 22. Above note 20 at p 4.  
 23. Section 6 of the Act.  
 24. Section 6 of the Act.

25. Part III of the Act is concerned with information privacy. Division 1 sets out what is meant by an interference with privacy. Section 13A deals with the interference of the privacy of individuals by organisations. See ss 6A (breach of an NPP if an act or practice is contrary to, or inconsistent with, that NPP) and 6B (breach of an approved privacy code if an act or practice is contrary to, or inconsistent with, the code). See further ss 13A(c) and (d), 13B, 13C, 13D and 13E.

26. Section 6C of the Act. In some instances, State instrumentalities and agencies or acts and practices thereof can be treated as that of an organisation: see ss 6F and 7A.

27. Section 6D(3) of the Act.

28. According to the definition in s 6 of the Act. What if your ODR service also provides a health service such as counselling online? Does this mean that the entire business falls within the definition?

29. What also of health information? During a dispute, an ODR provider may come across this sort of information, such as whether someone is HIV positive.

30. Sections 6D(7) and (8).

31. Office of the Federal Privacy Commissioner *Application of the Privacy Act to Information Already Held* Information Sheet 10 (2001) available at <[www.privacy.gov.au](http://www.privacy.gov.au)>.

32. Greenleaf G 'Enforcement of the Privacy Act: problems and potential' Privacy Law 2001 Conference Sydney 28–30 May 2001 available at <[www.bakercyberlawcentre.org](http://www.bakercyberlawcentre.org)>. See also Greenleaf G 'Tabula rasa: ten reasons why Australian privacy law does not exist' (2001) 24(1) *UNSW Law Journal* 262 at 266–68.

33. Available at <[www.privacy.gov.au/faqs/bf/q1\\_print.html](http://www.privacy.gov.au/faqs/bf/q1_print.html)>.

34. See ss 36–51 of the Act.

35. Section 18BI of the Act.

36. This includes injury to the complainant's feelings or humiliation suffered by the complainant: s 52(1A) of the Act.

37. Section 55A of the Act, which includes 'a determination made by an adjudicator for an approved privacy code'. See also s 54. The court is to deal by way of a hearing *de novo* the question of whether or not there has been an interference with the privacy of the complainant.

38. For a more detailed discussion of the problems surrounding making an application for remedies under the Act see Greenleaf 'Enforcement of the Privacy Act' above note 32.

39. This includes external territories: s 5A of the Act.

40. NPP 9.

41. See further Finkelstein R 'Protection of intellectual property in cyberspace: jurisdictional issues' (2001) 47 *Intellectual Property Forum* 8; Middleton G and About J 'Jurisdiction and the internet' in Fitzgerald et al above note 11 p 245; and Bygrave and Svantesson 'Jurisdictional issues and consumer protection in cyberspace: the view from down under' (2001) *CyberLRes* 12 available at <[www.austlii.edu.au](http://www.austlii.edu.au)>.

42. *Entores v Miles* [1955] 2 QB 327; *Reese Bros Plastics Ltd v Harmin-Sobelc Australia Pty Ltd* [1988] 5 BPR [97325].

43. *Macquarie Bank v Berg* [1999] NSWSC 526 (2 June 1999) BC9902857; *Gutnick v Dow Jones & Co Inc* [2001] VSC 305 (28 August 2001) BC200104980; *ACCC v Hughes* (2002) ATPR 41-863.

44. See Finkelstein above note 41 at pp 11 and 18; and Lim above note 5 at p 60.

45. In particular, equitable type remedies like injunctions that are available under the Act. See *Macquarie Bank v Berg* [1999] NSWSC 526 (2 June 1999) BC9902857 and comments by Finkelstein in above note 41 at p 17.

46. For example, the *Foreign Judgments Act 1991* (Cth) does not include the US; Forder J and Quirk P *Electronic Commerce and the Law* Wiley Brisbane 2001 p 49.



47. For example, the ACCC and OECD Committee on Consumer Policy. See Finch B 'Consumer protection on the internet' in Fitzgerald et al above note 11 p 257.

48. *Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters*, available at <[www.hcch.net/e/workprog/jdgm.html](http://www.hcch.net/e/workprog/jdgm.html)>.

49. As noted by Professors Forder and Quirk in above note 46 at p 243, there are still some sticking points:

... in relation to B2C [business to customer], the US Government has objected to language in the draft treaty that would give consumers the right to sue businesses in courts where the consumer lives. Business interests (including Microsoft, AOL and IBM) are pushing for a system which consumer protection and privacy issues would be resolved by businesses which run 'alternative dispute resolution' (ADR) systems that would largely seek to enforce contract or apply industry codes.

An example of how an international dispute resolution scheme can have effect and overcome these difficulties is ICANN's dispute resolution policy regarding the registration of domain names. For further discussion of this see Lim above note 5 at pp 509-42.

50. [2001] FCA 1062 (6 August 2001) BC200104454.

51. *ACCC v Hughes* (2002) ATPR 41-863; *ASIC v Matthews* [2000] NSWSC 392 (4 May 2000) BC200002743; *ACCC v World Netsafe Pty Ltd* [2000] FCA 1827 (8 December 2000) BC200007801.

52. [1999] NSWSC 526 (2 June 1999) BC9902857.

53. See Finkelstein above note 41 at p 11.

54. Some authors suggest that in cyberspace it may be that the marketplace is sovereign; see Katsh E, Rifkin J and Gaitenby A 'E-commerce, e-disputes, and e-dispute resolution: in the shadow of eBay law' (2000) 15 *Ohio State Journal of Dispute Resolution* 705 at pp 731-33.

55. See Clarke above note 3.

56. *Dispute Resolution and Information Technology: Principles for Good Practice* (Draft) NADRAC March 2002 under 'Forms of Information Technology' available at <[www.nadrac.gov.au](http://www.nadrac.gov.au)>.

57. For a detailed consideration of various best practice guidelines and a suggested model see Wentworth E 'Online dispute resolution: global issues and Australian standards' *Access to Justice: Litigation and ADR Online Twilight Seminar* 11 October 2001 Centre for Law in the Digital Economy Monash University. Submitted as an attachment to the *Submission of the Australian Banking Industry Ombudsman to: Dispute Resolution in Electronic Commerce Discussion Paper* available at <[www.nadrac.gov.au/aghomes/advisory/nadrac/ecommerce/EcommerceADRsub2.doc](http://www.nadrac.gov.au/aghomes/advisory/nadrac/ecommerce/EcommerceADRsub2.doc)>.

58. See Wentworth above note 57 at pp 14-16 and Bygraves above note 3 at pp 3-4. Similar language is used in the NADRAC Good Practice Model above note 56.

59. See, for example, ss 19N and 67ZA of the *Family Law Act 1975* (Cth) and s 15 of the *Farm Debt Mediation Act 1994* (NSW).

60. See further <[www.ftc.gov](http://www.ftc.gov)>. On the issue of whether to post a privacy policy or not, see Glaser S *To Post an Online Policy or Not?* available at <[www.gigalaw.com/articles/2001/pfv/glasser-2001-11-pfv.html](http://www.gigalaw.com/articles/2001/pfv/glasser-2001-11-pfv.html)>.

**PUBLISHING EDITOR:** Natalie D'Enyar **MANAGING EDITOR:** Elizabeth McCrone **PRODUCTION:** Kylie Gillon **SUBSCRIPTIONS:** \$445 per year including GST, handling and postage within Australia of 10 issues plus binder and index **SYDNEY OFFICE:** Locked Bag 2222, Chatswood Delivery Centre NSW 2067 Australia **TELEPHONE:** (02) 9422 2222 **FACSIMILE:** (02) 9422 2408 **DX** 29590 Chatswood [www.lexisnexis.com.au](http://www.lexisnexis.com.au) [natalie.denyar@lexisnexis.com.au](mailto:natalie.denyar@lexisnexis.com.au)

**ISSN 1440-4540 Print Post Approved PP 255003/03417 Cite as (2002) ADR 5(7)**

This newsletter is intended to keep readers abreast of current developments in alternative dispute resolution. It is not, however, to be used or relied upon as a substitute for professional advice. Before acting on any matter in the area, readers should discuss matters with their own professional advisers. The publication is copyright. Other than for purposes and subject to the conditions prescribed under the Copyright Act, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission.

Inquiries should be addressed to the publishers. Printed in Australia ©2002 LexisNexis Butterworths ABN: 70 001 002 357

