ADA

Australian Digital Alliance

PO Box E202, Kingston ACT 2604 T: (02) 6262 1273 F: (02) 6273 2545

ALRC Discussion Paper 72
Review of Australian Privacy Law

Submission of the
Australian Digital Alliance

December 2007

Submitted by email: privacy@alrc.gov.au

1. Introduction

This submission is made on behalf of the Australian Digital Alliance (ADA). The ADA thanks the Australia Law Reform Commission (ALRC) for the opportunity to comment on *Discussion Paper 72: Review of Australian Privacy Law* (the **Discussion Paper**).

The ADA is a non-profit coalition of public and private sector interests formed to promote balanced copyright law and provide an effective voice for a public interest perspective in the copyright debate. ADA members include universities, schools, consumer groups, galleries, museums, IT companies, scientific and other research organisations, libraries and individuals.

Whilst the breadth of ADA membership spans across various sectors, all members are united by the common theme that intellectual property laws must strike a balance between providing appropriate incentives for creativity against reasonable and equitable access to knowledge.

Digital developments, particularly in relation to enforcement of intellectual property rights, have lead to areas where there is an important intersection between intellectual property and privacy issues.

We set out our comments and recommendations in relation to these issues below.

2. Digital Rights Management (DRM)

The ADA wishes to draw particular attention to the effect that DRM technologies can have on privacy.[1] DRM technologies are used to control how material can be copied and even whether material can be accessed by the user. The Discussion Paper notes that privacy issues go hand in hand with virtually all DRMs. Not only do DRMs control the use of material, in most cases they also collect personal information about consumers. This might include tracking of consumer activities, such as how and when the content is accessed, but also tracking of surfing habits and even profiling consumer behaviour.

A well known example of this was seen in the Sony Rootkit controversy, where music CDs that contained DRM technology to prevent copying the CD contained software that constantly ran on the consumer's computer and collected information such as user listening habits. The technology also opened consumers' computers up to security breaches by third parties. This technology was hidden however and consumers had no ability to opt out of the information being collected.

Scope of "Personal Information"

A great deal of the information collected via DRMs would not fall within the current definition of "personal information". The ADA is strongly supportive of the

[1] We note that paragraphs 6.95 and 6.96 of the Discussion Paper specifically consider this issue.

recommendation[2] that the definition of "personal information" be broadened to include information such as IP addresses and surfing habits.

Bundled Consent

Consumers are very often subject to "bundled consents" in relation to DRMs. Products containing DRM technology often require a consumer to click "I agree" to *all* the terms and conditions, which include privacy provisions. These provisions can involve giving consent to collection of a broad range of personal information, and use of the consumer's information in a wide range of ways, including permission to pass information on to third parties. In many cases there is little justification (other than profiling or marketing) for the organisation to be collecting this personal information. For example in the case of a computer game that collects personal information via DRMs, this information is generally not required in order for the consumer to play the game.

The issue of providing bundled consent is particularly pertinent here as often the consumer *must* provide consent to all terms and conditions in order gain access to the product. The *Copyright Act* makes it an offence in most cases to break DRMs, so consumers cannot break the DRMs in order to gain access to the product without being required to consent to all the terms and conditions (including the collection of personal information). Kerr's piece on the privacy implications of DRMs in the US makes a point pertinent to Australia, saying: "If our laws are to prohibit people from circumventing the technologies that protect copyright, then they ought also to prohibit those same technologies from circumventing the laws that protect privacy" [3].

In their report on DRMs and privacy[4], the Canadian Internet Policy and Public Interest Clinic also revealed how frequently DRMs are coupled with collection of a large quantity of consumer's information that did not appear to be necessary to the service or product the organisation offered.

The Discussion Paper proposes[5] that the Office of the Privacy Commissioner provide further information and advice to organisations on when it is and is not appropriate to use "bundled consents". It is further proposed that organisations must not collect personal information unless it reasonably believes the information is necessary for one of its functions or activities.[6] It is unlikely that the first proposal will stop organisations from using bundled consents. However the ADA does support the second mentioned proposal, as this may assist in providing controls over the kind of information that organisations seek to collect via DRMs.

---

[2] Proposal 3-5 *Discussion Paper 72: Review of Australian Privacy Law* 31 July 2007. <http://www.austlii.edu.au/au/other/alrc/publications/dp/72/ >.

[3] Kerr, Ian "If Left to Their Own Devices…How DRM and Anti-Circumvention Laws Can Be Used to Hack Privacy." *In the Public Interest: The Future of Canadian Copyright Law*. Toronto: Irwin Law, 2005 at 210. <http://www.idtrail.org/content/view/173/42/>.

[4] Canadian Internet Policy and Public Interest Clinic. *Digital Rights Management Technologies & Consumer Privacy* September 2007. <http://www.cippic.ca/uploads/CIPPIC_Report_DRM_and_Privacy.pdf>.

[5] Proposal 16-1 *Discussion Paper 72: Review of Australian Privacy Law* 31 July 2007. <http://www.austlii.edu.au/au/other/alrc/publications/dp/72/ >.

[6] Ibid, Proposal 18-3.

Information collected

As mentioned previously, this information may currently be included in the general terms and conditions, meaning that in many cases the user is not properly made aware of the privacy implications of clicking "I agree" to those terms and conditions. The ADA is supportive of the proposed "Specific Notification" principles, requiring organisations to notify individuals in particular when they collect personal information[7]. This is an improvement on the existing principles that only require notification of the general type of information that the organisation might collect.

Technologically Neutral Terms

Proposal 7-1 states that the *Privacy Act* should be technologically neutral, to ensure that the Act remains flexible and relevant in the case of technological change. We note that, importantly, the Discussion Paper also suggests that specific provisions for technologies may be necessary where these technologies are known to raise particular privacy issues. This proposal does not mention DRMs, however we have shown some of the major privacy issues that DRMs raise and suggest this is an area where specific provisions should be included.

3. Information held by Internet Service Providers (ISPs)

At Paragraphs 8.1 and 8.2 Discussion Paper notes that ISPs hold and handle large quantities of personal information relating to their clients. This has increasing implications in the area of copyright. Copyright owners and rights holders across the world have been placing increasing pressures on ISPs and related bodies to reveal information about their clients in cases of suspected copyright infringement over the web, and to even take an active part in identifying copyright infringement by monitoring customers' behaviour.

In the US case of *RIAA v. Verizon*[8], ISP Verizon was taken to court by the Recording Industry Association of America (RIAA) for refusing to reveal the identity of a subscriber that the RIAA suspected of copyright infringement via peer to peer software. Verizon argued they needed to protect the privacy of its subscribers, and that it is not the job of ISPs to police copyright material contained on its subscribers' computers (as in this case). Although the court accepted Verizon's argument, the case illustrates how in the US the onus is placed on ISPs to defend releasing information about subscribers.

Another recent issue of concern in the US involved the Motion Picture Association of America (MPAA) attempting to persuade universities to install software to track the behaviour of university students on the university network in an attempt to pick up piracy.[9]

---

[7] Proposal 20-1 Proposal 18-3 *Discussion Paper 72: Review of Australian Privacy Law* 31 July 2007. <http://www.austlii.edu.au/au/other/alrc/publications/dp/72/ >.

[8] *RIAA v. Verizon Internet Services*, 543 U.S. 924, 125 S.Ct. 309 U.S. (2004).

[9] Krebs, Brian "MPAA University 'Toolkit' Raises Privacy Concerns" *Washington Post*. 23 November 2007.
<http://blog.washingtonpost.com/securityfix/2007/11/mpaa_university_toolkit_opens_1.html?nav=rss_blog>.

There is a certainly a need for the privacy principles to ensure that a person or organisation cannot obtain personal information simply by claiming to be a copyright holder suspecting a possible copyright infringement. As well as this, there is a need for regulation on the kind of information that ISPs are able to collect about their customers. The discussion paper doesn't consider this issue directly, but it is important to draw attention to the fact that the privacy principles should ensure that risk of possible infringement doesn't justify tracking of the consumer behaviour and the collection of personal information.

Small business exemption

An important issue the Discussion Paper raises is that the *Privacy Act* currently contains an exemption for small business, meaning they are not bound by privacy principles. The Discussion Paper notes that this means currently about 25% of ISPs aren't bound by privacy principles at all. The ADA strongly supports the suggestion that this exemption be removed. Ensuring that all ISPs are regulated by the Privacy Act is the first step to addressing the privacy concerns we raised above.

Other Comments

Our comments made under the preceding DRMs section in relation to the use of bundled consents, the definition of personal information, and the collection of information are also applicable to our comments on ISPs. We are supportive of the effect that these general proposals will have on how and when ISPs are able to collect information.

4. Privacy and Intellectual Property

Recent digital developments have led to a far greater amount of personal information that can be collected and used (or misused) by organisations. The ADA is concerned that copyright owners have abused their economic rights in the past and invaded the privacy of consumers and users of copyright law. In the face of significant digital developments, it's important to ensure that concerns about copyright infringement are adequately balanced with respect for privacy. As Kerr suggests[10]:

> If digital and network technologies increase the prospect of digital piracy, then our proposed solutions ought not to diminish the prospect of digital privacy. The legitimate goal of online anti-piracy protection must not succumb to the excessive and dangerous business of online anti-privacy protection.

The ADA thanks the ALRC for the opportunity comment. Please contact us should you have any further queries or would like further information.

Laura Simes
Executive Officer | Australian Digital Alliance
T: 02 6262 1273 | F: 02 6273 2545 | E: lsimes@nla.gov.au

[10] Kerr, Ian "If Left to Their Own Devices…How DRM and Anti-Circumvention Laws Can Be Used to Hack Privacy." *In the Public Interest: The Future of Canadian Copyright Law*. Toronto: Irwin Law, 2005 at 210. <http://www.idtrail.org/content/view/173/42/>.