LexisNexis™ Butterworths

Volume 9 Number 5
Print Post Approved 24437100049

Internet Law
Bulletin

Still trapped in the web: network administration and the Telecommunications (Interception and Access) Act 1979 (Cth)

Andrew Schatz AUSTRALIAN GOVERNMENT SOLICITOR

contents

This article discusses the amendments to the *Telecommunications (Interception) Act 1979* (Cth) (the TI Act) introduced by the *Telecommunications (Interception) Amendment Act 2006* (Cth) (the Amending Act). It also analyses the new telecommunications interception and access regime and its implications for employers and network administrators.

Parliament's primary concern in passing the Amending Act was to strike the right balance between empowering law enforcement agencies and protecting the privacy of personal communications during their passage over telecommunications systems.[1] According to the Explanatory Memorandum to the Amending Act (the EM), the telecommunications interception regime is intended to protect the privacy of personal communications by generally prohibiting the interception of communications, subject to certain limited exceptions where privacy is outweighed by other considerations.[2] Australian courts have also referred to this privacy objective on a number of occasions.[3]

The Amending Act amends the TI Act to implement certain recommendations of the *Report of the Review of the Regulation of Access to Communications* prepared by Anthony Blunn AO (the Blunn Report). Mr Blunn was asked to review policy options for the regulation of access to telecommunications, with a particular emphasis on new and emerging telecommunications technologies. The resulting Blunn Report, which is the fifth major report dealing with telecommunications interception legislation since 1994, was presented to Parliament on 14 September 2005.

It is also worth noting by way of introduction that the name of the TI Act changed to the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act) on 13 June 2006. The new title better reflects the fact that, while the TIA Act continues to govern the interception of telecommunications in Australia, it also establishes a warrant regime for enforcement agencies to access 'stored communications' held by telecommunications carriers.[4]

The principal amendments

The principal amendments introduced by the Amending Act:

- establish a regime to govern access to 'stored communications' held by telecommunications carriers (Sch 1: the Stored Communications Amendments);
- enable, in certain limited circumstances, the interception of communications of persons known to communicate with a 'person of interest' (Sch 2);

- enable, in certain limited circumstances, interception of telecommunications services on the basis of the use of a telecommunications device (Sch 3);
- remove the distinction between class 1 and class 2 offences, for which tele-communications interception powers are conferred on law enforcement agencies (Sch 4); and
- remove the Telecommunications Interception Remote Authority Connection function currently exercised by the Australian Federal Police, and transfer the associated warrant register function to the Commonwealth Attorney-General's Department (Sch 5).

This article focuses on the Stored Communications Amendments, which commenced on 13 June 2006.[5] The Stored Communications Amendments are of particular relevance to employers and network administrators that are responsible for operating and maintaining computer networks with internet and email facilities. This is because accessing, monitoring and/or recording email and internet traffic is an essential part of many filtering, quarantining, archiving, disaster recovery and professional standards-related practices.[6] Accordingly, any laws restricting the extent to which employers and network administrators can lawfully access or record communications are likely to have a significant impact on their capacity to maintain and protect their computer networks.

The new meaning of the term 'stored communications'

The Stored Communications Amendments are intended to preserve the distinction between accessing stored communications and intercepting real time communications as recommended in the Blunn Report (see the EM at p 4). However, the previous definition of stored communications inserted at s 7(3A) of the TI Act by the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* (Cth) (the Stored Communications Act)[7] has also been replaced by the following definition at s 5(1) of the TIA Act:

> ***stored communication*** means a communication that:
> (a) is not passing over a telecommunications system; and
> (b) is held on equipment that is operated by, and is in the possession of, a carrier; and
> (c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.

Accordingly, the term 'stored communications' no longer applies to all communications stored in any form other than on a 'highly transitory basis', and the new prohibition against 'accessing stored communications' only applies to communications that are accessed through a telecommunications carrier. According to the EM (at pp 4–5), this limitation expressly recognises the ability of enforcement agencies to continue using lawful access arrangements to access communications stored on devices that are accessible without the assistance of a telecommunications carrier (for example, through production by consent, a search warrant or a notice to produce).

The EM (at p 6) and the Supplementary Explanatory Memorandum (the Supplementary EM, at p 3) summarise the application of the new telecommunications interception and access regime as follows:

- communications that are 'passing over a telecommunications system' remain subject to the general prohibition against interception (s 7 of the TIA Act);
- communications that are 'stored communications' are subject to the new prohibition against accessing stored communications (s 108 of the TIA Act); and
- communications that are not passing over a telecommunications system and are not 'stored communications' (because they are not accessed through a telecommunications carrier) remain subject to general principles of lawful access including consent, general search warrants and notices to produce.

There is no specific reference to the ability of employers or network administrators to access communications held on equipment they possess and operate in the EM, the Supplementary EM or the Second Reading Speech. However, by implication, the new provisions of the TIA Act permit employers and network administrators to lawfully access and record communications held on equipment they possess and operate at any time, except when the communications are 'passing over a telecommunications system'.

The new 'stored communications warrant' regime

Chapter 3 of the TIA Act establishes the general prohibition against accessing 'stored communications', subject to certain limited exceptions. Section 108(1) of the TIA Act states that a person commits an offence (punishable by a penalty including imprisonment up to two years) if:

(a) the person:
  (i) accesses a stored communication; or
  (ii) authorises, suffers or permits another person to access a stored communication; or
  (iii) does any act or thing that will enable the person or another person to access a stored communication; and
(b) the person does so with the knowledge of neither of the following:
  (i) the intended recipient of the stored communication;
  (ii) the person who sent the stored communication.

However, s 108(2) of the TIA Act provides, among other things, that s 108(1) does not apply to:

(a) accessing a stored communication under a stored communications warrant; or
(b) accessing a stored communication under an interception warrant.

A number of concerns were raised about the new stored communications warrant regime during the relevant Parliamentary and Senate Committee debates including the lower threshold for, and broader access to, stored communications warrants compared to telecommunications interception warrants.[8] However, the government responded by emphasising the higher threshold for stored communications warrants compared to the standard search warrants used during the 18 months prior to 13 June 2006, as well as the additional record-keeping and reporting requirements introduced to promote accountability.[9]

The difference between 'accessing' and 'intercepting'

Section 6AA of the TIA Act defines the term 'accessing a stored communication' to mean:

> … listening to, reading or recording such a communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication.

By comparison, s 6(1) of the TIA Act retains the following TI Act definition of 'intercepting a communication passing over a telecommunications system':

> … listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

It is unclear why the definition of 'accessing a stored communication' includes 'reading' but the definition of 'intercepting a communication passing over a telecommunications system' does not. However, the distinction may be of little consequence, given the impracticality of reading a communication passing over a telecommunications system without creating a copy.[10]

It is also worth noting that the two definitions differ in terms of whose knowledge matters for the purpose of determining whether or not the interception or accessing is unlawful. Section 108(1)(b) of the TIA Act only prohibits accessing a stored communication with '… the knowledge of neither of the following':

(i) the intended recipient of the stored communication;
(ii) the person who sent the stored communication.

Accordingly, s 108(1)(b) permits lawful access to stored communications without a warrant provided the sender, the intended recipient, or both of those parties know in advance that the stored communications will be accessed.[11] It is unclear why the general prohibition against interception of communications is not equally limited, given the impracticality of notifying all potential senders of communications in advance that their communications may be intercepted prior to delivery while in transit.[12] It is also unclear why the definition of 'accessing a stored communication' does not refer to both the sender and intended recipient in a manner consistent with s 108(1)(b).

The new concept of 'passing over a telecommunications system'

The Stored Communications Amendments are intended to clarify when a communication is 'passing over a telecommunications system'.[13] To that end, s 5F(1) of the TIA Act states that a communication:

(a) is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication; and
(b) is taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication.

However, s 5F(2) alters the position with respect to communications sent from addresses on computer networks operated by or on behalf of the Australian Federal Police (AFP) for a period of two years from 13 June 2006. Such communications are not taken to start passing over a telecommunications system for the purposes of the TIA Act until they are no longer under the control of any of the following:

(a) any AFP employee responsible for operating, protecting and maintaining the network;
(b) any AFP employee responsible for enforcement of the Professional Standards of the Australian Federal Police.

The references to 'operating, protecting and maintaining the network' and 'enforcement of the Professional Standards of the Australian Federal Police' recognise the operational difficulties that could arise if the AFP and its network administrators were unable to lawfully access (or intercept) a

communication sent from a telecommunications device within an AFP computer network before the relevant communication reached its network boundary (the Gateway). In fact, the Supplementary EM states (at p 3) that the insertion of s 5F(2) 'will enable lawful access to those communications for the AFP within the AFP network boundary'.

However, while the AFP has been granted the right lawfully to access and record outgoing communications at or prior to its Gateway for operational, security, maintenance and professional standards purposes, a similar right has not been extended to employers and network administrators more generally. Accordingly, all organisations (except the AFP) should review their policies and network administration practices to ensure they do not authorise or engage in behaviour that is unlawful under the new telecommunications interception and access regime.

In particular, if there is a need to access or copy outgoing communications at or prior to a Gateway, then organisations should ensure their employees and other network users are adequately informed in advance. Carefully drafted and promulgated policy documents will help, but regular reinforcement through online screen prompts and user training sessions may also be required.[14]

Determining when a communication is 'accessible to its intended recipient'

It is necessary to consider when a particular communication becomes 'accessible to its intended recipient' to determine whether it is 'passing over a telecommunications system'. To that end, s 5H(1) provides that a communication is accessible to its intended recipient if it:

(a) has been received by the telecommunications service provided to the intended recipient; or
(b) is under the control of the intended recipient; or
(c) has been delivered to the telecommunications service provided to the intended recipient.

The application of s 5H(1) is fairly straightforward with respect to clearly defined telecommunications services provided by carriers such as home dial-up internet, and email services. However, the position is more complicated with respect to communications sent to intended recipients at electronic addresses on corporate computer networks (for example, the work email address of an employee of a business or government agency).

In one view of the matter, the 'telecommunications service' provided in such a case could constitute the entire network that enables the intended recipient to access communications passing over external telecommunications systems operated by telecommunications carriers (that is, all lines and equipment comprising the telecommunications network from the Gateway to the relevant telecommunications device used by the intended recipient). According to this view, all incoming communications would cease passing over the relevant telecommunications system at the Gateway of the relevant destination network. Accordingly, the communications would no longer be subject to the general interception prohibition and the organisation or administrator responsible for operating the network could lawfully access and record the incoming communications at the Gateway.

However, a court would consider that allowing organisations to intercept communications at the Gateway to a computer network would contravene the privacy objectives of the TIA Act,[15] particularly in view of the provisions set out in s 5G, as discussed directly below.

Identifying the 'intended recipient' of a communication

Section 5G(1) of the TIA Act defines the term 'intended recipient' as follows:

(a) if the communication is addressed to an individual (either in the individual's own capacity or in the capacity of an employee or agent of another person) — the individual; or
(b) if the communication is addressed to a person who is not an individual — the person; or
(c) if the communication is not addressed to a person — the person who has, or

> whose employee or agent has, control over the telecommunications service to which the communication is sent.

Accordingly, in the case of a communication sent to the electronic address of an employee or other user on a corporate network, the TIA Act provides that the communication continues to pass over the telecommunications system until it becomes 'accessible to' the individual user to whom the relevant communication is addressed (see the EM at p 6).

In addition, s 5G(2) of the TIA Act was inserted to provide a specific definition of 'intended recipient' for communications sent to an electronic address on a computer network operated by or on behalf of the AFP. The Supplementary EM (at p 4) explains the effect of the new provision as follows [emphasis added]:

> The effect of the amendment will be *to enable the AFP to intercept (copy) all e-mail communications received at the AFP network boundary before they are received by the individual intended recipient*. Unlike all other organisations, the AFP will therefore be able to access these communications without warrant [sic] before they are received by the intended recipient. This is to ensure the maintenance of the AFP's Professional Standards.
> *All other organisations will be prohibited from accessing stored communications without a warrant until such time as they are received by the intended recipient*, thereby ensuring that only communications that have been delivered to, are under the control of, or are accessible by the intended recipient may be accessed without warrant [sic].

The extracted portion of the Supplementary EM is difficult to reconcile with the actual wording of s 5G(2) of the TIA Act.[16] However, the provisions themselves strongly argue in favour of a construction that ensures communications continue to 'pass over a telecommunications system' until they are able to be physically accessed by their intended recipient, even if the intended recipient does not access them right away. According to this view, an incoming email sent to an individual user on a corporate network would only complete its passage over the telecommunications system when it arrived at the destination mail server and was capable of being accessed by its intended recipient.

The AFP's special rights to lawfully access and record incoming communications at its Gateway appear intended to complement the legislative reforms introduced by *Law Enforcement (AFP Professional Standards and Related Measures) Act 2006* (Cth), which received Royal Assent on 30 June 2006.[17] The government is also aware of the conflict between the general prohibition against interception of communications and the need to allow other organisations and network administrators to lawfully access and record communications passing over their computer networks.[18] Accordingly, the AFP's special rights appear to be an interim measure and the government is yet to determine a long-term solution to the conflict between the general interception prohibition and the operational needs of employers and network administrators.[19]

Further amendments to the TIA Act may be made during Parliament's 2006 spring sitting.[20] However, in the meantime, it is important that all organisations (other than the AFP) realise that the amendments introduced by the Stored Communications Act on 14 December 2004 are no longer effective. As a result, such organisations should review their IT security and acceptable use policies as well as their network administration practices, to ensure they do not authorise or engage in behaviour that is unlawful under the new telecommunications interception and access regime.[21]

Concluding remarks

Given Parliament's primary concern with striking the right balance between empowering law enforcement agencies and protecting the privacy of personal communications, it is perhaps unsurprising that the operational needs of employers (other than the AFP) and network administrators have not been

specifically addressed. The government's long-term solution to the conflict between the general interception prohibition and lawful access rights for the purpose of network administration is yet to be revealed. In the meantime, the telecommunications interception and access regime remains in a state of flux and organisations should continue to review their policies and practices at regular intervals to account for the ongoing changes in communications technology and the laws that govern it. ●

Andrew Schatz, Senior Lawyer, Australian Government Solicitor, Adelaide.

Endnotes

1. See Explanatory Memorandum to the Amending Act at p 9 and Parliament of Australia *Parliamentary Debates: House of Representatives (House of Representatives Hansard)* (Hon Philip Ruddock MP, Attorney-General) 16 February 2006 at p 10.
2. See the EM at p 9.
3. *Edelsten v Investigating Committee of NSW* (1986) 7 NSWLR 222 at 229 (Lee J); *R v Edelsten* (1990) 21 NSWLR 542 at 548 (CCA); *T v Medical Board* (SA) (1992) 58 SASR 382 at 398 (Matheson J; Debelle J agreeing); *Green v The Queen* (1996) 124 FLR 423 at 432 (Franklyn J; Pidgeon and Rowland JJ agreeing).
4. *House of Representatives Hansard* 16 February 2006 (Hon Philip Ruddock MP) at pp 7–8.
5. See Amending Act, Sch 1.
6. See Schatz A 'Trapped in the web: IT policies and the Stored Communications Act' (2005) 8(3) *INTLB* 33 at 34 for further examples of circumstances where network administrators may require access to email and internet communications passing over their networks.
7. Above.
8. *House of Representatives Hansard* 28 February 2006 at pp 95–96 (per Duncan Kerr MP), 1 March 2006 at p 2 (per Peter Garrett MP) and pp 8–9 (per Daryl Melham MP); *Parliamentary Debates: Senate (Senate Hansard)* 28 March 2006 at pp 85–86 (per Sen Natasha Stott Despoja).
9. See *House of Representatives Hansard* 1 March 2006 at pp 12, 14 (per Philip Ruddock MP) and *Senate Hansard* 28 March 2006 at pp 93, 124 (per Hon Sen Chris Ellison, Minister for Justice and Customs).
10. The act of opening and viewing an email on a computer monitor usually involves the automatic creation of a 'Pagefile' record of all or part of the email, which can be subsequently retrieved and viewed until such time as it is 'written over'.
11. *Senate Hansard* 29 March 2006 at pp 131–132 (per Sen Chris Ellison, Sen Joe Ludwig and Sen Natasha Stott Despoja); *Senate Hansard* 30 March 2006 at pp 2–4 (per Sen Chris Ellison, Sen Joe Ludwig and Sen Natasha Stott Despoja).
12. Above note 6, p 34.
13. See the EM at p 6 and Supplementary EM at p 3.
14. See above note 6, p 36 for an action checklist setting out some of the issues to be considered during any such policy review.
15. Above note 4 and the EM at p 9.
16. The extracted text twice refers to organisations other than the AFP being unable to access communications without a warrant 'before they are received by the intended recipient'. However, an ordinary reading of the provisions suggests that a more accurate explanation would be: 'All other organisations will be prohibited from *intercepting* incoming communications before they become *accessible to* their intended recipient'.
17. *Senate Hansard* 29 March 2006 at pp 125–129 (per Sen Chris Ellison, Sen Joe Ludwig and Sen Natasha Stott Despoja). In particular, see Sen Chris Ellison's comments at p 126.
18. Above at pp 125–126 (per Sen Chris Ellison).
19. See above and Supplementary EM at p 4.
20. *Senate Hansard* 28 March 2006 at pp 93, 117 (per Sen Chris Ellison).
21. Above note 6.

ICANN cans plans for .xxx domain: what happened?

Jaime Riffel and **Ryan Gilchrist**
MADDOCKS LAWYERS

For the last six years, the Internet Content Management Registry (ICM Registry) has campaigned for the registration of a '.xxx' Top Level Domain (TLD), which would be dedicated to the adult entertainment industry. ICM Registry proposed that the establishment of a .xxx domain would support the voluntary relocation of responsible adult entertainment sites from various TLDs to .xxx, where the sites would be monitored to ensure compliance with certain standards. The plan, if given the go-ahead, would have effectively enabled registrants to purchase domain names like <red.xxx>.

The campaign involved ICM Registry submitting an application for the .xxx domain to the Internet Corporation for Assigned Names and Numbers (ICANN), based on the selection criteria for new sponsored TLDs and the value of the proposal as a proof-of-concept. The application was approved by the ICANN board in June 2005. However, on 10 May 2006, the ICANN board reversed its decision by voting against the proposal to enter into a registry agreement with ICM Registry.

This article outlines the proposal to establish the .xxx domain in the context of some of the public policy issues.

Categorisation of .xxx

There are various types of TLDs within the Domain Name System (DNS).[1] A generic TLD (gTLD) is a form of TLD which is linked to a particular category or organisation.[2] gTLDs can further be categorised as either 'sponsored' or 'unsponsored'. As its name suggests, the sponsored TLD has a sponsor which is responsible for representing a part of the community that is most affected by the operation of the TLD.

The .xxx TLD is categorised as a sponsored gTLD that specifically represents the online adult entertainment community. The sponsor organisation for the .xxx TLD, the International Foundation for Online Responsibility (IFFOR), was delegated the authority to formulate policies in relation to the way in which the .xxx TLD would operate for the benefit of its defined group of stakeholders. As the policy-making body for the .xxx TLD, an important objective of the IFFOR was to foster the communication between the responsible online adult entertainment community and the wider internet community.

Why was .xxx proposed?

The application was submitted in response to ICANN's plans to expand the DNS name space.[3] There were numerous reasons put forward in support of .xxx, including the proposed benefits of providing a better mechanism for filtering access to explicit sites.[4] Nevertheless, the economic factors should not be overlooked as a large motivating reason for the campaign.

It is reported that ICM Registry intended to charge a wholesale price of around US$60 per year for a .xxx domain name which could then be marked up by resellers.[5] Accordingly, had ICM Registry's plans for the .xxx domain succeeded, not only would it have generated a large sum of money, but it would also have controlled the rights to some of most lucrative online assets.

Arguments for .xxx

The .xxx TLD was primarily intended to be used to balance the competing interests between those who wish to provide and access sexually explicit material on the internet, and those who wish to avoid access to it. Arguments for .xxx have mainly centred on the idea that the domain would provide a tool for easier filtration of pornography and regulation.

Some of the benefits of the .xxx TLD that were proposed by ICM Registry and the IFFOR include the following.

- The promotion of Best Business Practices, integrated into the .xxx registration agreement, within the online adult entertainment community. This would help to regularise business procedures and ensure that a responsible approach was taken by adult entertainment providers.
- The development of a filtering system for individuals or households wishing to prevent access to adult content. The .xxx TLD would make it easier for parents and employers to block the entire TLD.
- The introduction of a self-regulated forum for all stakeholders to discuss and react to concerns about online adult entertainment. This would promote the domain's aim to combat child pornography.

Arguments against .xxx

During a period of public comment on ICM Registry's proposal, many concerns were raised in opposition to .xxx. Some of these concerns include the following.

- The voluntary nature of the .xxx TLD would not compel internet providers of sexually explicit material to use the .xxx TLD. This would mean that sexually explicit material would still be available in other domains. Consequently, the domain's aim to restrict access to sexually explicit material could appear to be useless.
- Registrants of existing adult sites might attempt to duplicate their registrations in the .xxx domain in order to compete with the registration of sought-after names that were unavailable in other TLDs.
- The introduction of an identifiable area of the internet for pornographic websites would generate a 'virtual red light district' and thereby legitimise the online adult entertainment industry.
- The establishment of the .xxx domain could drive governments to legislate for the mandatory relocation of all existing adult entertainment sites to

this domain,[6] which in turn, could challenge ideas about freedom of expression and censorship laws.

Evaluation of .xxx application: how events unfolded

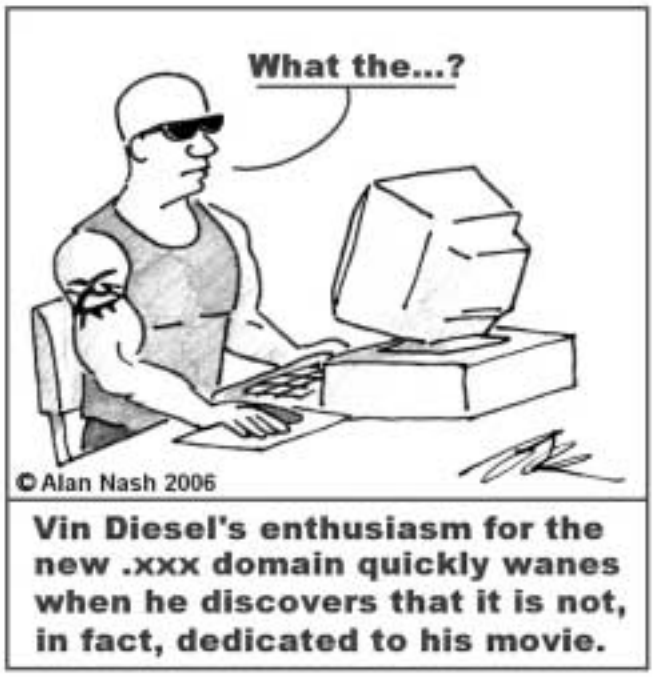
In November 2000, an independent evaluation team reviewed ICM Registry's application against the selection criteria established by ICANN. The evaluation team rejected the application partly on the grounds that it failed to meet 'unmet needs'. This was because adult content was readily available on the internet and there was no mechanism requiring adult content to move from existing TLDs to the .xxx TLD.[7] Additional concerns relating to privacy and the First Amendment were also raised by the general public of the US, signifying the degree of controversy surrounding .xxx and a reluctance to recommend its selection.

In May 2004, the .xxx application was again subjected to an independent review carried out by three independent evaluation teams (the Team).[8] The Team's report stated that the application met the technical and financial criteria but lacked clarity in relation to the sponsored community and public interest criteria outlined in the sponsored TLD selection criteria.

The primary difficulty the team encountered in its evaluation was the lack of consistency in the definition of 'adult-oriented information'. ICM Registry had proposed to serve a community of registrants that would be associated with this type of content. However, the Team found that, due to the moral, religious, national and cultural perspectives involved, the content category was not 'susceptible to [an] objective, globally-applicable definition'.[9] There was also concern that the IFFOR's dual responsibility of serving the interests of its sponsored community as well as the interests of privacy and child advocacy would lead to a dilution of either or both of these interests.[10]

In June 2005, the board of ICANN resolved the uncertainty expressed by the Team, and approved the application on the basis that the .xxx application met the relevant selection criteria. The board subsequently directed the staff of ICANN to enter into commercial negotiations with ICM Registry for the registry agreement.

In March 2006, the Governmental Advisory Committee (GAC) of ICANN met to clarify the process by which ICANN was to enter into negotiations with ICM Registry. The GAC questioned the reasoning that was applied by the ICANN board in approving the application, and requested a written explanation with regard to the sponsored community and public interest criteria.[11] In response to this meeting, although the ICANN board expressed its reservations about whether it would be appropriate to proceed with entering into the registry agreement with ICM Registry,[12] it nonetheless believed that such concerns could possibly be addressed by contractual obligations in the registry agreement.[13] In May 2006, ICANN announced that the board had voted against entering into any further negotiations for the proposed registry agreement with ICM Registry.[14]



Current status

Since the rejection of the .xxx proposal, ICM Registry has filed a motion of reconsideration to ICANN in relation to the vote of its board. In the request for reconsideration, ICM Registry has claimed that 'Members of the Board voted against the ICM Agreement based on inaccurate information about the written statements of various governments concerning .xxx'.[15]

ICM Registry has also filed an action in the US District Court, against the US Department of Commerce and the Department of State, for injunctive relief with respect to violation of the *Freedom of Information Act* (US).[16] ICM Registry believes that the government departments possess uncensored copies of official documents which may expose the extent to which the US government influenced ICANN's consideration of the .xxx application.[17]

Reflection on controversy surrounding .xxx

The final decision of the ICANN board may have further ignited the controversy that has surrounded the related subject matter of the .xxx domain. The public has been left to ponder questions relating to what constitutes 'adult content', and how sites promoting such information should be effectively regulated, in order to balance the interests of users who seek to select with those who seek to avoid adult entertainment sites. Undoubtedly, issues of censorship and the problems with governing pornography across jurisdictional boundaries are also brought into this equation.

Some of the debates about the .xxx domain have been inherently political in nature because of the high demand for governments to consider the multitude of moral, religious and cultural perspectives of the public. Furthermore, the subjective tests that have been involved in determining the appropriateness of the .xxx domain

have drawn attention to the significant responsibilities of ICANN in relation to internet governance and public policy decision-making. ICANN's decision to effectively abandon the .xxx proposal has raised interesting questions about the value of independent review of TLD applications and the function of governments in representing the diverse range of public policy concerns. The .xxx application demonstrates how the traditional role of ICANN, in managing the technical coordination functions for the internet, can be challenged by issues of public policy which impact on the overall governance of the internet. ●

Jaime Riffel, Lawyer, and Ryan Gilchrist, Lawyer, Maddocks Lawyers, Sydney.

Endnotes

1. The Internet Assigned Numbers Authority (IANA) currently subdivides TLDs into three categories: country code TLDs (ccTLDs), generic TLDs (gTLDs) and infrastructure TLDs (the TLD '.apra' is the only domain confirmed). See the IANA website at <www.iana.org/domain-names.htm>.

2. For example, '.com' is used for commercial organisations and '.jobs' is used for employment-related sites.

3. Other applications submitted in response to ICANN's plans for expansion of the DNS namespace included '.mobi' (for sites catering to mobile devices) and '.post' (for postal services).

4. It is beyond the scope of this paper to discuss whether the .xxx domain would have provided a more efficient means of filtration other than the methods currently available.

5. Special Broadcasting Service (SBS) World News Australia 'Cyber-Space Red Light District' 3 June 2005, at <www9.sbs.com.au/theworldnews/region.php?id=113040&region=4>.

6. For example, on 16 March 2006, US Senators Max Baucus and Mark Pryor introduced a Bill that would require websites that contain 'material that is harmful to minors' to operate from a new TLD: Boyer Q 'Senators Baucus and Pryor author Bill to create mandatory adult TLD,' *Free Speech Coalition* 16 March 2006, at <www.freespeechcoalition.com/FSCView.asp?coid=272>. Full text of Bill available at <www.freespeechcoalition.com/documents/GRA06387finalintroversion_xml1.pdf>.

7. ICANN *Report on TLD Applications*: *Application of the August 15 Criteria to Each Category or Group* 9 November 2000, at <www.icann.org/tlds/report/report-iiib1c-09nov00.htm>.

8. These comprised the Technical Team, the Business/ Financial Team and the Sponsorship and Other Issues Team.

9. Williams L, Ouedraogo P and Weitzner D (Sponsorship and Other Issues Team for ICANN) 'New sTLD Applications' *Appendix D — Evaluation Reports: Evaluation Report prepared for the Internet Corporation for Assigned Names and Numbers (ICANN)* Section III: 'Report of the Sponsorship and Other Issues Team' 28 November 2005 at 110, available at <www.icann.org/tlds/stld-apps-19mar04/PostAppD.pdf>.

10. Above at 111.

11. ICANN GAC Meeting 'Final Communique' Wellington, NZ 28 March 2006 at 3, available at <http://gac.icann.org/web/communiques/gac24com.pdf>.

12. Letter from Dr Paul Twomey, President and CEO of ICANN, to Chairman and Members of ICANN GAC 4 May 2006, at <www.icann.org/correspondence/twomey-to-tarmizi-04may06.pdf>.

13. Above.

14. 'ICANN board votes against .xxx sponsored top level domain agreement' 10 May 2006, at <www.icann.org/announcements/announcement-10may06.htm>.

15. ICM Registry, 'Amended request for reconsideration of board action' 19 May 2006 at 2, at <www.icmregistry.com/ReconsiderationRequestComplete.2.pdf>.

16. *ICM Registry LLC v US Dept of Commerce and US Dept of State* Complaint for Injunctive Relief for Violation of the *Freedom of Information Act*, US DoCC case no 1:06CV00949, 19 May 2006 at 2, available at <www.icmregistry.com/DoCComplaintAsfiled.pdf>.

17. Above.

Casenote

NILESH MEHTA v J PEREIRA FERNANDES SA
[2006] EWHC 813 (Ch)

This is an English High Court case on appeal from a District Court judgment enforcing a personal guarantee, on the basis that an email satisfied the requirements for writing and signature under the *Statute of Frauds Act 1677* (UK) (the Act), which is the legislation governing personal guarantees. The appellant submitted that he should not be liable under the guarantee, on the basis that there was no signed agreement. The respondent argued that the email constituted the agreement, and the existence of the sender's email address in the email header constituted a signature.

Facts

Mr Mehta was a director of Bedcare (UK) Ltd. The company failed to pay one of its suppliers, J Pereira Fernandes SA (JPF) and ultimately was wound up by petition by JPF. The winding up petition was made by JPF on 12 January 2005. On this date, Mr Mehta asked a member of his staff to send an email to the solicitors of JPF, requesting that the hearing of the petition be adjourned, subject to a personal guarantee being given by Mr Mehta in favour of JPF for the amount owing by Bedcare. This email was not signed by Mr Mehta, but the header showed that the email had come from <Nelmehta@aol.com>. No further steps were taken to formalise the guarantee, and Mr Mehta did not pay any amount to JPF.

JPF commenced proceedings against Mr Mehta to recover the amount owing by Bedcare, relying on the email of 20 February. On 9 November 2005, District Court Judge Harrison gave a summary judgment in favour of JPF. Mr Mehta was ordered to pay the amount of the personal guarantee plus costs. The current case is an appeal by Mehta again the judgment.

Issues

Section 4 of the Act requires that a memorandum or note of personal guarantee must be in writing and signed by the party guaranteeing, or by some other person authorised by them. There were two key legal issues on appeal. The first was whether the email constituted a sufficient 'memorandum or note' which could form the basis of a guarantee in accordance with the Act. Assuming the email was a sufficient note, the second issue was whether it was sufficiently signed by Mehta.

Was the email a sufficient memorandum or note?

The Appeal Court began on the assumption that the email was not a sufficient note or memorandum to satisfy the Act, because the words of the email appeared to constitute a proposal, rather than an agreement.[1] However, Judge Pelling QC went on to consider various cases that supported the proposition that an offer signed by one party and orally accepted by the other was a sufficient note or memorandum of guarantee.[2] The Appeal Court applied this authority in the present case, since it was not disputed that the email was in writing and that the offer was orally accepted by JPF.

Did the email address in the header constitute a signature?

The Appeal Court accepted the proposition that an email address appears automatically in the header of an email. The respondent relied upon *Evans v Hoare*[3] to support an argument that an email address is sufficient to constitute a signature for the purposes of the Act. The respondent argued that, by authorising an employee to send an email from his email account, Mehta knew that his email address would be visible to the recipient, and that the email address therefore constituted a signature for the purposes of the Act.

His Honour, however, relied on dicta in *Caton v Caton*[4] in finding that, whatever letters or numbers appeared as a signature on a document, the Act was satisfied only if they were included in order to give authenticity to the document. *Caton*'s case involved a document that, although not signed, started by referring to the 'under mentioned parties' and proceeded to refer to the parties by name in relation to various promises. In *Caton*, the House of Lords held that the document did not satisfy s 4 of the Act. Lord Westbury found that:

> ... the mere circumstances of the name of a party being written by himself in ...(an) ... agreement will not of itself constitute a signature. It must be inserted in the writing in such a manner as to have the effect of "authenticating the instrument" or "so as to govern the whole instrument ...[5]

Outcome

Judge Pelling QC examined the purpose of the Act, which he believed to be to protect people from being held liable on the basis of informal communications, and found that the purpose of the Act would be undermined if the email address was found to constitute a sufficient signature in this case.

The court held that, while the email constituted a sufficient note or memorandum of guarantee, the automatic assertion of the email address in the particular circumstances of Mehta's case did not constitute a signature. The appeal was therefore allowed. ●

Ed Gomes, Solicitor, and Danielle Roth, Paralegal, Freehills, Sydney.

Endnotes

1. Cave J in *Evans v Hoare* [1892] 1 QB 593 held that the memorandum must be one of contract, not merely one of proposal.
2. *Lever v Koffler* [1901] Ch 543; *Hussey v Horne-Payne* (1879) 4 App Cas 311; *Parker v Clark* [1960] 1 WLR 286.
3. See above note 1.
4. (1867) LR 2 HL 127.
5. Above at 143.

bytes

ACCC releases a guide to the advertising and promotion of internet services

As a result of the increase in complaints against internet service providers (ISP) the ACCC has released a guide relating to the advertising and promotion of internet services. The key areas focused on include the promotion of broadband services, costs associated with call connections and help lines, and the wording of advertisements and disclaimers.

The guide is easy to navigate and contains many practical and real-life examples where advertisements have been in breach of the legislative provisions.

Free and unlimited products

When advertising a product, the ISP must be cautious when using terms such as 'free' and 'unlimited'. Where ISPs make statements relating to future matters or the provision of free products, there must exist a reasonable basis or expectation that the service is capable of being provided. Where a service is 'free' it must not be subject to payment of any kind, and any additional conditions related to the product or service must be clearly and prominently drawn to the attention of consumers.

Unlimited broadband means unlimited by speed, volume of download or time. All representations made regarding performance and speed will be misleading and deceptive unless they are capable of being met, at both peak and off-peak times.

Pricing

Pricing of internet services was also seen as an area of concern. Particular issues covered included price bundling, cancellation and upgrade fees, and call connection costs. The legislation imposes obligations on ISPs to make clear to customers all aspects of cost associated with the provision of services. Where prices are subject to bundling, this should be clearly communicated to the customer. Where there is a restriction on the usage of the internet service, specifically in remote or rural areas, customers must be made aware of instances where their connection costs may be subject to long distance call costs.

The 2003 case of *ACCC v Dodo Internet Pty Ltd* was used as an example (see <www.accc.gov.au>). Here, Dodo was prosecuted for misleading and deceptive conduct as a result of an advertisement for dial-up internet, which stated that customers would be provided with unlimited internet access for the cost of a local call. Some customers incurred long-distance call rates when they signed up with Dodo. By consent an injunction was granted against Dodo to cease making the claims.

Usage policies

Usage policies are relevant in the event that an ISP believes that a customer is taking advantage of an unlimited or free offer. Where such policies are in place, ISPs must ensure that customers are fully informed of the terms prior to entering into contracts.

The ACCC requires that customers be given adequate information in order to accurately compare products. Terms and conditions of contract must be clearly explained, particularly in the event that there exists a clause which allows the company to alter prices, terms and conditions at any time and for any reason. The minimum obligations require customers to be fully informed of the existence and exercise of such clauses.

Disclaimers

ISPs should not use disclaimers, qualification or fine print to correct a misleading impression created by a more prominent aspect of an advertisement. Disclaimers should be used only to clarify the meaning or the intent of the statement. In order to be effective the disclaimer must be sufficiently prominent, easily readable in its context, proximate and clear in its meaning.

<Fair.com>, a guide to advertising and promoting internet services, is a helpful and easy-to-read guide outlining the practises that ISPs should adopt when advertising products and services to their customers. ●

Yvonne Vukosav, Articled Clerk, Blake Dawson Waldron, Melbourne.

A précis of piracy on the PC: results of a worldwide piracy study

Australia has a software piracy rate of 31 per cent, resulting in US$361million in losses last year, according to the 2005 *Global Software Piracy Study* published by the Business Software Alliance (BSA) and the International Data Corporation (IDC).

In the third annual study of its kind, the *Global Software Piracy Study* examined the use of all packaged software that runs on personal computers, such as operating systems, business applications and games. Although it found that the average world-wide piracy rate of 35 per cent in 2005 was the same as in 2004, this masks a number of underlying trends.

For example, piracy rates in the developing world far exceed those in the developed world. The countries with the worst piracy rates are Vietnam (90 per cent), Zimbabwe (90 per cent) and Indonesia (87 per cent), whereas the countries with the lowest piracy rates are the US (21 per cent), NZ (23 per cent) and Austria (26 per cent). Australia ranks 14th lowest, with a 31 per cent piracy rate. Australia's piracy rate has remained fairly constant on average over the past three years. However this is against the background of an expanding IT market.

Developed countries usually have bigger markets in IT, resulting in bigger losses. For example, although the US had the lowest piracy rate, it suffered the largest losses, at US$6,895million last year. In general, the study confirms that piracy across the world remains a significant issue. It found that for every two dollars spent on personal computer software, one dollar's worth was obtained illegally.

There are huge benefits to be gained from reducing piracy. IDC and BSA found that if the global rate is reduced by 10 per cent over four years, then 2.4 million new jobs would be created, and there would be an extra US $70 billion in tax revenues to local governments. However, there are some trends on the horizon that could mean rises in piracy.

For example, India, China and Russia have some of the world's worst piracy rates, but are also huge growth markets in IT. The study also points out that peer-to-peer networks on the internet are a significant factor in piracy rates. With 60 per cent of internet traffic driven by peer-to-peer downloads, and the introduction of 100 million new internet users by the end of this year (and the fastest growing internet populations coming from countries with high piracy rates), then the stage is set for some real piracy issues.

What can be done? The study points out that reducing global piracy is a complex task. Factors such as culture, industry trends, even geography can have a role to play. However, the study makes five suggestions aimed at country-wide changes:

- countries should adopt the Copyright Treaty established by the World Intellectual Property Organization;
- stronger copyright enforcement mechanisms need to be put in place, such as those in the World Trade Organization's Trade-Related Aspects of Intellectual Property Rights Agreement (TRIPS);
- improve enforcement by providing enforcement agencies with better resources, and encouraging cross border cooperation between agencies;
- increase public education programs; and
- government agencies, as the largest users of personal computer software in the world, should lead by example.

For further information, see <www.bsa.org/globalstudy> or <www.bsaa.com.au/bsaaweb/main/index.php?pg=media_single&PID=117&ch_table=link7>. ●

Scott Smalley, Solicitor, Freehills, Melbourne.

YouTube sued for infringement of copyright

A Los Angeles journalist has commenced proceedings in the US District Court against the operators of the phenomenally successful YouTube video sharing site for infringement of copyright in a video recording of the 1992 Los Angeles riots. In the statement of claim, Robert Tur has alleged that the video was posted without his consent and was viewed more that 1000 times by users of the popular site. The footage, which was filmed by Tur's wife, Marika Tur, from a helicopter, shows truck driver Reginald Denny being attacked during the 1992 Los Angeles riots. YouTube Inc has defended its site, claiming that it is a service provider that complies with the *Digital Millennium Copyright Act* (US) and that it is protected under the safe harbour provisions of that Act.

Followers of the recent spate of online copyright cases (Napster, Grokster, Kazaa, Cooper) have been expecting a challenge to the YouTube site for some time. The site, which has been in operation for the past 18 months, allows users to post videos without any pre-screening process. YouTube first came under public scrutiny earlier this year when a clip from NBC's 'Saturday Night Live' show was removed, following complaints from NBC. Although the majority of files uploaded by users do not infringe third party rights, there is a large quantity of copyright material, such as television clips and music videos, which is available for viewing only (this is in contrast to other sites which have been the subject of copyright infringement proceedings which permit downloading of files).

It will be interesting to see the outcome of the YouTube decision and the court's comments on sharing of copyright material in the context of the YouTube site architecture. Of particular significance will be the 'notice and takedown' system to respond to infringement notices from copyright owners, which YouTube has implemented. ●

Arthur Artinian, Lawyer, Blake Dawson Waldron, Sydney.

PUBLISHING EDITOR: Bridget Brooklyn BA (Hons) PhD **MANAGING EDITOR: Anupama Bhattacharya PRODUCTION: Jane Farrugia**
SUBSCRIPTION INCLUDES: 10 issues per year plus binder SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067 Australia
TELEPHONE: (02) 9422 2222 FACSIMILE: (02) 9422 2404 DX 29590 Chatswood www.lexisnexis.com.au bridget.brooklyn@lexisnexis.com.au
ISSN 1329-9735 Print Post Approved PP 244371/00049 Cite as (2006) 9(5) *INTLB*