You Can't Always Get What you Warrant

Kieran Mahony and Tara Walker consider the conflict between protection of information under Australian law and disclosure compelled by overseas laws

Introduction

Individuals and companies involved in the supply of telecommunications in Australia are subject to a general requirement to protect the confidentiality of subscriber information and the content of communications under the regime for protection of communications contained in Part 13 of the *Telecommunications Act 1997* (Cth) (the ***Telecoms Act***). The prohibition on disclosure is subject to various exceptions, which are set out in Division 3 of Part 13.

Carriers and Carriage Service Providers (***CSPs***) also have obligations under the *Telecommunications (Interception and Access) Act 1979* (Cth) (***Interception Act***) in respect of access to and use of 'stored communications'.

This article considers a hypothetical dilemma in which an Australian Internet Service Provider (***ISP***), with operations located in the United States, is served with a warrant to produce information by an American law enforcement agency, for example the Federal Bureau of Investigation (***FBI***), requiring disclosure of confidential information in circumstances that are not covered by the exceptions and therefore could involve breach of Australian law (***FBI Scenario***). A company in such a situation would potentially be forced to choose between breaching Australian law or facing contempt charges or other consequences in the jurisdiction in which the warrant is issued.

Companies may be able to avoid or minimise the risk of encountering this problem. In particular, terms and conditions of standard customer agreements can be drafted to try and bring confidential information within the ambit of knowledge or consent disclosure exceptions in the legislation.[1] The extent to which this approach adequately shields companies from liability is considered below.

The issue also justifies attention from the communications regulator, the Australian Communications and Media Authority (***ACMA***). The industry would benefit from guidance as to how to deal with this situation (or avoid it in the first place).

How and why the problem arises

Accessing confidential information in Australia - policy context

The extent to which law enforcement agencies should be allowed access to confidential information in the interests of law enforcement and national security has been the subject of much debate in contemporary legal and political discourse. Heightened security concerns are often relied upon by governments to justify changes in the balance between the privacy rights of individuals and the investigative and enforcement capabilities of the state.[2]

The many security and privacy implications stemming from the increasing flow of information across borders have also been widely considered at an international level.[3] Australian law clearly recognises that there are circumstances in which it will be desirable to compromise the confidentiality of private information in the interests of security, including where that information is in the possession of non-Australian telecommunications carriers operating in Australia. The tension between security and privacy concerns is manifested in the dichotomy between the general prohibition against disclosure of confidential information in Division 2 and the exceptions in Division 3 of Part 13 of the Telecoms Act. The content of Part 13 of the Telecoms Act, along with relevant provisions in the Interception Act in relation to 'stored communications', will be considered in greater detail below.

Despite the apparent potential for this conflict of obligations to arise, there is little guidance for companies as to how to deal with the problem. This is presumably a reflection of the fact that the problem simply was not anticipated when the legislation was drafted.[4]

Intersection of laws

Although not considered in the telecommunications legislation, the conflict issue has been contemplated in other related areas. Notably in the Australian context, the *Privacy Act 1988 (Cth)* (***Privacy Act***) states in section 13D that:

> *An act or practice of an organisation done or engaged in outside Australia and an external Territory is not an interference with the privacy of an individual if the act or practice is required by an applicable law of a foreign country*.[5]

Frustratingly for telecommunications operators, this provision does not protect them, as Part 13 of the Telecoms Act operates concurrently with the Privacy Act. The recently released Australian Law Reform Commission report on Australian Privacy Law and Practice (***ALRC Privacy Report***) notes several submissions calling for a more consistent approach to privacy regulation in the field of telecommunications.[6] Suggestions to the ALRC included that Division 3 be removed from Part 13 and to allow the Privacy Act to solely regulate the exceptions field, or that Part 13 be completely moved into the Privacy Act. Nevertheless, the ALRC Privacy Report concludes that both Acts should continue to separately regulate privacy in the telecommunications industry, on the grounds that it is appropriate for the use and disclosure of the particular type of information covered by Part 13 (i.e. subscriber information and the contents of communications) to be subject to more stringent rules than those in the Privacy Act.[7]

Protection of communications under the Telecoms Act

The Telecoms Act does not refer specifically to ISPs, but applies to them because they fall within the category of carriage service providers.[8] CSPs supply communications services to the public using carrier infrastructure. Part 13 aims to protect privacy in communications by restricting CSPs (including ISPs), carriers, telecommunications contractors and their respective employees ('eligible persons')[9] from using or disclosing information relating to:

a) the contents of communications that have been, or are being, carried by carriers or CSPs (delivered or not); and

b) carriage services supplied by carriers and CSPs; and

c) the affairs or personal particulars of other persons.[10]

Electronic communications such as emails and instant messages may contain information falling within at least two of these categories: they contain both content of communications (the body of the email or message), and personal particulars of both subscribers and the recipients of their communications, such as identity, source, path and destination details. Emails are stored and forwarded 'at successive points along their journey to a nominated address', with the final point in the journey being the recipient's ISP computer or mail server, where they reside until accessed by the recipient.[11]

With regards to Australian ISPs with servers located and operated outside Australia by third party contractors, the extra-territorial application of the Telecoms Act[12] means that these servers fall within the ambit of Part 13.

Eligible persons must not use or disclose any information or document that relates to any of the three categories mentioned above and that came to their knowledge or into their possession in the course of carrying on their businesses.[13] Subject to the exceptions (discussed below), use or disclosure in contraven-

tion of this section is an offence punishable on conviction by imprisonment for a term not exceeding 2 years. [14]

Exceptions

The prohibitions against disclosure in Part 13 of the Telecoms Act are subject to a number of exceptions as set out in Division 3 of that Part. Whilst these are extensive,[15] they do not appear to apply in a situation such as the FBI Scenario, leaving Australian ISPs exposed to the risk of a conflict between complying with their obligations under Part 13 and relevant laws overseas.

The exceptions include situations where the use or disclosure is: made by an employee in the performance of duties for the carrier as employer;[16] required or authorised under an *Australian* warrant or *Australian* law;[17] made to ACMA or the Australian Competition and Consumer Commission (***ACCC***) to assist in carrying out their functions and powers,[18] made with the knowledge or consent of the person concerned;[19] made with the implicit consent of the sender and recipient of the communication;[20] for prescribed business needs of other carriers or service providers;[21] or permitted under the regulations.[22]

Disclosure authorised by or under law

As mentioned, it appears that these exceptions only apply where the authorisation or requirement is under Australian law.[23] Paragraph 280(1)(a) permits disclosure or use in connection with the operation of an enforcement agency, where the disclosure or use is required or authorised under a warrant. 'Enforcement agency' has the same definition as in the Interception Act and appears to be limited to Australian enforcement agencies.[24] The second limb of the exception (in paragraph 280(1)(b)) relates to disclosure or use required or authorised by or under law, and this is presumably limited to Australian law.

Under the Privacy Act, by contrast, if an organisation:

> *reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles*

then it may transfer personal information to someone who is in a foreign country.[25] Further, an act or practice of an organisation done or engaged in outside Australia and an external Territory is not an interference with the privacy of an individual if the act or practice is required by an applicable law of a foreign country.[26]

As identified by the ALRC, it is doubtful whether sections 280 or 297 of the Telecoms Act would allow a telecommunications service provider (such as an ISP) to rely on the more expansive exceptions of the Privacy Act *in addition to* those exceptions contained in the Telecoms Act. [27] Even if they did, not all ISPs would be caught by the Privacy Act due to the small business exception;[28] and in any event, compliance with Part 13 is a carrier licence condition, so would arguably need to be complied with by carriers irrespective of the operation of the Privacy Act.[29]

The ALRC has also recommended an additional exception under Part 13 for circumstances where a person 'has reason to suspect that unlawful activity has been, is being, or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.'[30] If such an exception were introduced, eligible persons finding themselves in a position analogous to the FBI Scenario could potentially seek to utilise it to justify 'reporting its concerns to relevant persons or authorities' such as the FBI. Query, however, whether this exception is intended for persons who actively initiate their own investigations, as opposed to those who are merely responding to and assisting with the investigation of another body. Query also whether 'relevant persons or authorities' could be read as extending to a foreign law enforcement agency.

Consent exceptions

An alternative means by which an Australian ISP could deal with a situation such as the FBI Scenario is to use its standard terms of service and/or privacy policy to try and bring itself within one of the consent options under Division 3.[31] Section 289 states that disclosure or use by a person of information or a document will not be prohibited if:

> *a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and*
>
> *b) the other person:*
>
> *(i) is reasonably likely to have been aware or made aware that information or a document of that kind is usually disclosed, or used, as the case requires, in the circumstances concerned; or*
>
> *(ii) has consented to the disclosure, or use, as the case requires, in the circumstances concerned.*

Section 290 contains an 'implicit consent' exception. It provides that disclosure or use is not prohibited if:

> *(d) the information or document related to the contents or substance of a communication made by another person; and*
>
> *(e) having regard to all of the relevant circumstances, it might reasonably be expected that the sender **and** the recipient of the communication would have consented to that disclosure or use, had they been aware of the disclosure or use.*

The contrasting language used in these two sections reflects the distinction between the two main types of information protected under this Part. The 'affairs or personal particulars' referred to in section 289 covers subscriber information (for example the names, addresses and other details of customers). The 'contents or substance of a communication' referred to in section 290 pertains to the actual information contained in a communication (for example the contents of emails or SMS messages).

Different thresholds apply to each of these exceptions. For the disclosure of subscriber information (section 289), the carrier need only show that the customer is 'reasonably likely to have been aware or made aware that information or a document of that kind is usually disclosed' in the circumstances. In the FBI Scenario, this requirement might be satisfied if the ISP's terms of service or standard customer agreement included a provision to the effect that confidential information will be handed over to a law enforcement agency – domestic or otherwise – in circumstances where it is validly sought under applicable legislation from the ISP or a related company.

In their respective privacy policies applicable to the provision of email services, ISPs such as Microsoft[32], Google[33] and Yahoo!7,[34] all include terms whereby subscribers must consent to the transfer, storage and processing of personal information on servers located outside the country in which they reside. These policies also contain terms reserving the ISP's rights to access personal information in limited circumstances, including where a reasonable belief is held that disclosure is necessary to comply with applicable laws and process. Read together, these terms arguably provide a basis upon which the ISPs can argue that they have obtained the implicit consent of the subscriber, at least in respect of accessing subscriber information.

For the disclosure of the content of a communication, the threshold is higher. To be covered by the exception in s 290, the carrier must show that:

> *it might reasonably be expected that both the sender **and** the recipient of the communication would have consented to the disclosure or use, if they had been aware of the disclosure or use*.

The extent to which this exception applies may again depend on the standard terms and conditions issued by the individual ISP, however the difficulty is establishing that the recipient of the communication (who is not a party to the agreement) of the communication implicitly agreed to the disclosure.

Protection of communications under the Interception Act

Carriers and CSPs also have obligations under the Interception Act in respect of access to and use of 'stored communications'.[35] The definition of 'stored communication' has a number of elements. The communication must:

- not be passing over a telecommunications system (it is only stored once it has ceased passing over a system - communications in the process of passing may not be intercepted without a warrant, or unless some other exception applies);
- be held on equipment operated by, and in the possession of, a carrier; and
- 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.[36]

'Carrier' in this context is defined to include a CSP. While this would include an Australian ISP, it may not extend to include a foreign company operating a server located overseas on behalf of the ISP. If an overseas warrant were issued seeking content held on a server or equipment owned by the Australian ISP, but operated in the relevant overseas jurisdiction by a third party contractor, it is possible that content would not actually constitute 'stored communications' because it would not be 'held on equipment operated by and in the possession of' the Australian ISP.

Carriers and CSPs who are in possession of stored communications within the meaning of the Interception Act are obliged under subsection 108(1) of the Interception Act not to:

a) access a stored communication; or

b) authorise, suffer or permit another person to access a stored communication; or

c) do any act or thing that will enable the person or another person to access a stored communication,

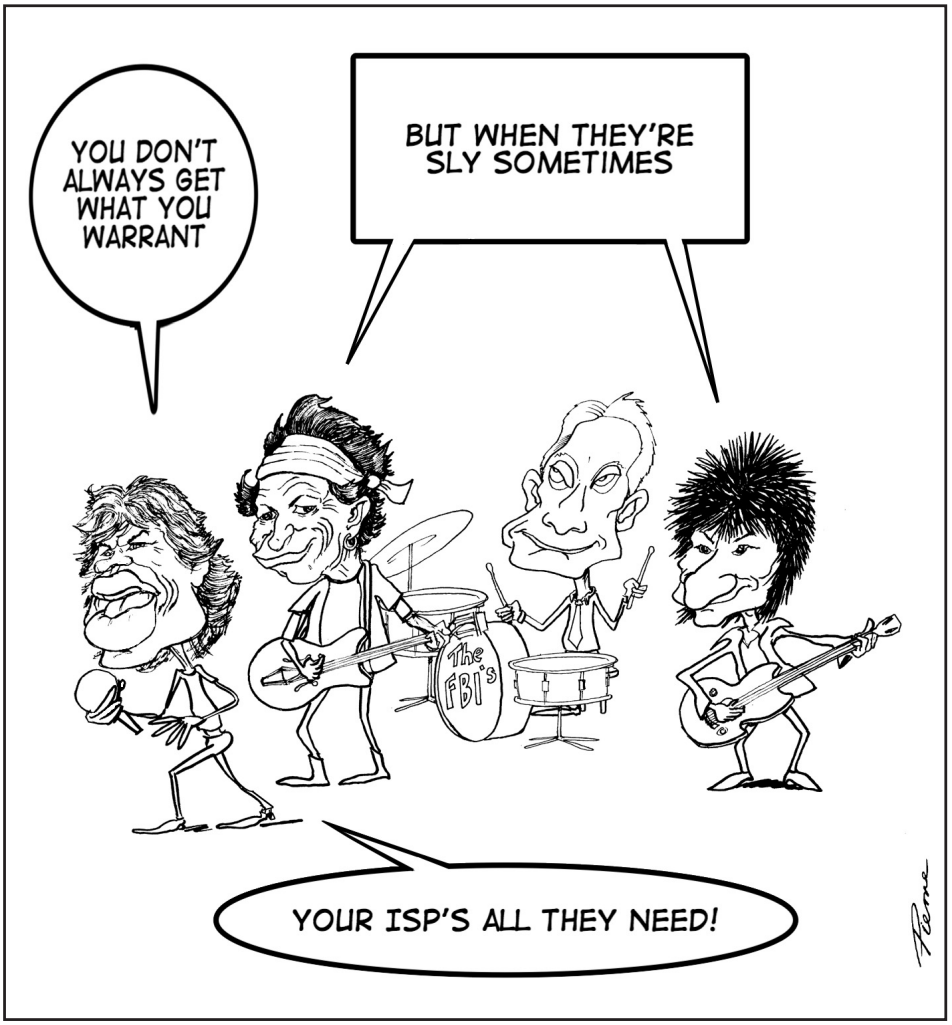
without the knowledge of the intended recipient of the stored communication and the person who sent the stored communication.

A person is taken to have 'knowledge' if they are given written notice of an intention to access. This appears to entail written notice of an intention to do a *specific* act or thing, rather than a general notice as to the possibility of access occurring at some stage. Accordingly, the 'knowledge' requirement may not be satisfied simply by an ISP including a general access provision in its customer terms and conditions. However, a subscriber to an email or messaging service is presumably the intended recipient of messages in the 'inbox', and the sender of messages in the 'sent mail' box. In this light, a specific written notice to the relevant subscriber could possibly satisfy the knowledge requirement.

Breach of section 108 of the Interception Act is punishable on conviction by imprisonment for 2 years or 120 penalty units ($13,200) or both.

Exceptions

Subsection 108(2) of the Interception Act contains a number of exceptions to the obligations set out in subsection 108(1), including exceptions relating to warrants issued under the Interception Act, the activities of



Australian law enforcement agencies, and where access is reasonably necessary to perform a person's duties (relating to installation, connection or maintenance of equipment etc). None of these exceptions appear to apply in circumstances where a warrant is issued in another jurisdiction for access to the content of a communication classified as a stored communication for the purposes of the Interception Act.

How the FBI Scenario may be dealt with in practice

The ISP may be assisted by the relevant mutual assistance agreements between Australia and the United States as a means of legitimately exchanging the necessary information.[37] A formal request for the information in question by the Australian authorities, pursuant to an arrangement with their US counterparts, would appear to bring the disclosure under the law enforcement exception in section 280 of the Telecoms Act. It appears that analogous situations are commonly dealt with in this way.

Assuming any breach was identified by ACMA and referred to the Commonwealth Department of Public Prosecutions (***CDPP***), the circumstances may not support the taking of further action by the CDPP. As outlined above, there are 'common sense' alternatives available to resolve the problem, and the CDPP's guidelines indicate that relatively trivial matters, or minor breaches of a 'technical' nature, will not meet the requisite public interest threshold for prosecution.

Conclusion

The FBI Scenario raises a technical legal point along with some interesting policy issues. The potential for conflicting legal obligations to arise for Australian ISPs operating abroad is presumably an unintended result of the overlap of the legislative regimes of different jurisdictions (and an inherent deficiency within that the regimes as the problem was not foreseen), combined with the rapid globalisation of telecommunications and associated increase in trans-border information exchanges. Anecdotal information suggests that ACMA and the Attorney-General's Department (which administers the Interception Act) are aware of the issues and perhaps should consider providing general guidance on the issue. As outlined in this paper, such measures include the use of appropriately drafted terms and conditions to bring potential disclosures of confidential information within the ambit of the legislative exceptions, or alternatively seeking the involvement of the Australian authorities under the relevant bilateral mutual assistance arrangements.

Kieran Mahony and Tara Walker are Lawyers at Clayton Utz in Sydney

(Endnotes)

1 Refer to sections 289-290 of the Telecoms Act. Matching secondary disclosure exceptions (by persons authorised to receive such information under Division 3) are contained in Division 4, sections 296-303A.

2 In Australia, this shift is arguably reflected in various pieces of legislation, for instance the *Anti-Terrorism Act 2005 (Cth)*.

3 See, e.g., the Asia-Pacific Economic Cooperation (***APEC***) Privacy Framework, the Organisation for Economic Co-operation and Development (***OECD***) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the European Parliament and the Council of the European Union (***EU***) Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

4 The opposite scenario could presumably also occur - where a non-Australian operator with activities in Australia could find itself in breach of its own domestic regulations - if it complies with disclosure requirements of Australian law enforcement agencies.

5 See also subsection 6A(4), which states that the National Privacy Principles are not breached by an act or practice required by an applicable law of a foreign country.

6 ALRC Privacy Report, Chapter 71 'Telecommunications Act', paragraphs 71.44 - 71.46.

7 ALRC Privacy Report, Chapter 71 'Telecommunications Act', Id, paragraphs 71.49-71.50.

8 Australian Communications and Media Authority, *Internet Service Providers and Law Enforcement and National Security Fact Sheet*, accessed on 22 July 2007 at http://www.acma.gov.au/WEB/STANDARD?pc=PC_100072

9 Telecoms Act, s 271.

10 Telecoms Act, s 276(1)(a).

11 T Starey, 'Getting the message: law enforcement agencies' access to stored communications' (2005) 10(1) *MALR* 25.

12 Telecoms Act, s 9.

13 Telecoms Act, sub-s 276(2).

14 Telecoms Act, sub-s 276(3).

15 It has recently been argued that the exceptions 'permit uses and disclosures of personal information for a broader range of purposes than the National Privacy Principles' which 'can result in diminished protections for personal information in the telecommunications sector', Office of the Privacy Commissioner, 'Submission to ALRC Review of Privacy', Issues Paper 31 (February 2007), p 396. Available at http://www.privacy.gov.au/publications/alrc280207.html

16 Telecoms Act, s 279.

17 Telecoms Act, ss 280 and 297 (secondary disclosure).

18 Telecoms Act, s 284.

19 Telecoms Act, s 289.

20 Telecoms Act, s 290.

21 Telecoms Act, s 291.

22 Telecoms Act, s 292.

23 Similarly, s 313 of the Telecommunications Act (which provides that a carrier is not liable for damages for an act done or omitted in good faith to give reasonably necessary assistance to officers and authorities of the Commonwealth, States, or Territories) applies only in relation to Australian law.

24 Interception Act, section 5. Note that the definition lists a number of Australian enforcement agencies (a) - (m), but also includes '(n) any body whose functions include administering a law imposing a pecuniary penalty.' There is no suggestion however that this would extend to foreign law enforcement bodies.

25 National Privacy Principle 9.

26 Privacy Act, s 13D.

27 See ALRC Privacy Report, paragraphs 72.27 - 72.30. Note that the ALRC has recommended amending sections 280 and 297 to clarify that the exception does not authorise a use or disclosure that would be permitted by the Privacy Act if that use or disclosure would not otherwise be permitted under Part 13 of the Telecoms Act (ALRC Privacy Report, Recommendation 72-1). Interestingly, section 303B provides for the reverse: disclosure or use permitted under Part 13 is taken to be authorised for the purposes of the privacy legislation.

28 See ALRC Privacy Report, paragraphs 39.52 - 39.57, which identifies the telecommunications industry as a 'high-risk sector' due to the large number of ISPs who fall within the small business exception based on a turnover of less than $3 million per annum.

29 Telecoms Act, Schedule 1.

30 ALRC Privacy Report, Recommendation 72-2.

31 Telecoms Act, ss 289 and 290.

32 Microsoft Online Privacy Statement: http://privacy.microsoft.com/en-au/fullnotice.aspx

33 Google Privacy Policy: http://www.google.com/privacypolicy.html

34 Yahoo!7 Terms of Service: http://au.docs.yahoo.com/info/terms/ and Yahoo!7 Privacy Policy: http://info.yahoo.com/privacy/au/yahoo/

35 Interception Act, s 108.

36 Interception Act, s 5.

37 Refer to the CDPP website page on 'international work': http://www.cdpp.gov.au/Practice/International.aspx. The formal mutual assistance regime relies on a network of international relations, and the goodwill of countries to assist each other in the investigation and prosecution of criminal matters. It is governed by the Mutual Assistance in Criminal Matters Act 1987. The United States has a 'Treaty with Australia on Mutual Assistance in Criminal Matters'. The formal regime runs parallel with a less formal system of international cooperation between investigating agencies.

Australian Domain Name Policy

Rebecca Sadleir discusses the new auDA policy and the relaxation of rules on transferring .au domain name licences

auDA, the Australian Domain Name Administrator, has introduced a policy which removes most of the restrictions which previously applied to the transfer of *.au* domain name licences from one person to another. The procedure for transferring *.au* domain names has also been simplified. The Transfers (Change of Registrant) Policy (2008-08) (the ***Policy***) came into effect on 1 June 2008.

auDA is the government-endorsed policy authority and industry self-regulatory body for the *.au* domain space. It is responsible for developing and implementing policies in relation to the *.au* domain space, as well as accrediting and licensing domain name registrars and facilitating the .au Dispute Resolution Policy. auDA also represents Australia at ICANN – the Internet Corporation for Assigned Names and Numbers, the organisation which co-ordinates the naming systems for the internet – and other international forums.

Background

There are no proprietary rights in a *.au* domain name, and it is not strictly possible to 'sell' a domain name. This is because a registrant does not 'own' the name itself; instead, it holds a licence to use the domain name for a specified period, subject to certain terms and conditions. However, it is possible to transfer a domain name licence in certain circumstances, and it is this which is addressed by the new auDA Policy.

Historically, both the registration and transfer of domain name licences in the *.au* space have been subject to strict controls. Although restrictions have gradually been eased over the last few years, the rules were (and indeed still are) significantly more stringent than those for domain names in many other countries and, for example, in the *.com* space.

Before the implementation of the Policy, transfer of a *.au* domain name licence was permitted only in specific, limited, circumstances. For example, it was not possible to transfer a domain name from one entity to another for purely commercial reasons, unless in the context of a wider business sale. In addition, the transfer process was relatively cumbersome and, amongst other things, required the transferee to make a statutory declaration confirming that the circumstances of the transfer complied with the relevant rules.