LOST IN TRANSCRIPTION: THE AUSTRALIAN REGIME FOR INTERCEPTION OF, AND ACCESS TO, COMMUNICATIONS CONTENT AND METADATA

ROB NICHOLLS[1] AND MICHELLE ROWLAND[2] **(Refereed)**

Abstract

In this paper, we discuss the European model for the interaction between agencies and telecommunications operators and analyse the application of this model for stored communications in the Australian regulatory context. We draw out the complexities in, and problems with, the Australian regime to show that the system has significant legal obscurities. We analyse the source of obligations to provide communications content and provide some criticism on the distinct lack of clarity which arises in the provision of communications content and metadata. We consider the practical approaches taken by Australian operators in the face of this uncertain regulatory regime. We conclude by suggesting some amendments to the regime which would provide the 'bright line' clarity which we argue is required in respect of a best practice interception and access regime.

Introduction

This paper takes a practical approach to the *Telecommunications (Interception and Access) Act 1979* which is associated with lawful interception of telecommunications and stored communications. Although lawful interception of voice communications has been practised for many years, there is an increasing demand from law enforcement agencies for access to other forms of communication. In 2006, this led to amending legislation which permitted certain agencies to gain access to stored communications by allowing access to each of emails, short message service messages and instant messages. In 2007, the scope of access to communications metadata was increased significantly. Arguably the most significant change in Australia in recent years is the new obligations to provide access to communications content and metadata under the *Telecommunications (Interception and Access) Act 1979*. This paper discusses the implications that arise from the changes in requirements for access to communications and the practical implementation of such access.

There are a significant number of obligations on carriers and carriage service providers to deliver communications metadata (including near real-time location information) to relevant agencies. These obligations arise from both law and contract. The relevant agencies utilise the regime far more extensively than their counterparts in other countries, a fact that should lead to a requirement for clear rights and responsibilities for operators and agencies. In practice, however, the Australian regime is both complex and, if misinterpreted, more intrusive than similar regimes in other OECD countries. The paper describes some practical cases which have affected carriers and carriage service providers and the response made by those operators to demands (whether or not supported by warrants) imposed by law enforcement agencies. We

[1] Rob is a consultant at Gilbert + Tobin and a PhD candidate at UNSW. He can be contacted at rnicholls@gtlaw.com.au or +61 2 9263 4023

[2] Michelle is a lawyer at Gilbert + Tobin. She can be contacted at mrowland@gtlaw.com.au or +61 2 9263 4223

then present an analysis of the issues that arise from these case studies, propose how the regime might be amended and draw conclusions.

Previous studies

The need for appropriate and lawful interception of voice communications has been recognised for the past fifty years, if only because of the lawlessness of interception in the first half of the twentieth century (Branch 2003). In Australia, the focus from 1960 to 2005 was only on regulating the interception of voice. There were some doubts about the legality of access to stored communications (for example, emails) and agencies obtained data either by a search warrant or an interception warrant (Holland 2004). However, the increasing options for communications, the potential for criminals to use communications mechanisms such as instant messaging (Nolin 2006) and the lack of security of this technology (Williams and Ly 2004) has led to a change in the Australian legislation. This change created a difference in the regulatory approach to live communications compared with stored communications (Bronitt and Stellios 2006; Nicholls and Rowland 2007).

Australia is not alone in changing the legislative and regulatory environments to attempt to address new technologies. South Africa took a simple approach and described communications as either 'direct' or 'indirect' and provided an interception regime for both (Bawa 2006). In the USA, there was debate about the more prescriptive and proscriptive approaches in the amendments to the *Communications Assistance for Law Enforcement Act* (US) (**CALEA**) which now encompasses internet-based communications environments and services (Schwaderer 2007). The debate included input from some of the original architects of the internet (Landau 2005; Bellovin, Blaze et al. 2006). Although this debate argued that there were technical as well as social risks to amending CALEA, the technical standards for emerging technologies already provided lawful interception access ports (Miettinen 1999; Milanovic, Srbljic et al. 2003; Milanovic, Srbljic et al. 2003; Street 2003; Fonknechten, Ghribi et al. 2004; Open Mobile Alliance 2005; Gidari 2006; Gratzer, Naccache et al. 2006; ETSI 2007).

Much of the focus of the debate on interception capability has been in respect of Voice over Internet Protocol (**VoIP**) (Drinan, Fontaine et al. 2005; Miller, Levine et al. 2005; Del Bianco 2006). Whereas the amendment to CALEA to introduce an obligation for interception of VoIP services was a new obligation, this is not the case in Australia.

The *Telecommunications (Interception and Access) Act 1979* imposes an obligation on all carriage service providers with facilities in Australia to maintain an interception capability (in section 191) and to provide assistance to relevant agencies (in Part 4). Another significant effect of the legislative amendments in 2007 was the movement of the obligations on carriers and carriage service providers from the *Telecommunications Act* 1997 (Cth) to the *Telecommunications (Interception and Access) Act 1979*. The prohibitions on disclosure of communications and communications metadata remain in sections 276–278 of the *Telecommunications Act* 1997 but the *Telecommunications (Interception and Access) Act 1979* sets out circumstances where these prohibitions no longer apply (as summarised in section 171). There remains in Part 14 of the *Telecommunications Act* 1997 an obligation on carriers and carriage service providers to give authorities such help as is reasonably necessary for the purposes of (among other things) enforcing the criminal law.

The European model

The European Telecommunications Standards Institute (**ETSI**) has developed a model for the interaction between law enforcement agencies and carriers or carriage service providers. There are three broad interfaces between telecommunications operators and law enforcement agencies and these are set out in (ETSI 2007).

As described by the authors previously (Nicholls and Rowland 2007), service provider interfaces with the law enforcement agency (**LEA**) on three levels. The first level, referred to as handover interface 1, is simply the administrative arrangements between the LEA and the service provider and is an ongoing relationship. In Australia, this may be a service agreement and service level agreement with the relevant LEAs. In other countries, this administrative interface is far more standardised and has, as a result, a higher level of transparency. The second level, referred to as handover interface 2, is the mechanism by which the service provider delivers communications metadata but not the content of communications. Typically, in Australia, this information is provided as part of the carriage service provider's 'reasonable assistance' obligations under the *Telecommunications Act* 1997 set out above. This type of information would include, in respect of an identified individual, the addresses or phone numbers of communications to and from that individual, information as to the time of the communication and limited information as to its nature (for example, the duration of a voice call or the size of an email). The final level, referred to as handover interface 3, is the mechanism by which the service provider delivers communications content to the LEA. In Australia, this material is delivered in response to a warrant.

This model provides a useful means to consider the development of interception and access over time. The model is general enough to be applicable to both voice and non-voice communications. It is also able to distinguish between communications metadata and the content of those communications.

Issues with stored communications

The *Telecommunications (Interception and Access) Act 1979* contains a general prohibition on the interception of stored communications in the same manner as telecommunications interceptions are prohibited in section 108 of the *Telecommunications (Interception and Access) Act 1979*. It also provides for certain exceptions in which a stored communication can be intercepted. These include where access is authorised by a stored communications warrant, where access is authorised by an interception warrant and certain other specific circumstances in section 108(2) of the *Telecommunications (Interception and Access) Act 1979*.

Relevantly for our discussion, a 'stored communication' is defined to mean a communication with all of the three specific elements prescribed in section 5 of the *Telecommunications (Interception and Access) Act 1979*:

- is not passing over a telecommunications system;
- is held on equipment that is operated by, and is 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.

The concept of 'passing over' is clarified within the *Telecommunications (Interception and Access) Act 1979* by providing that a communication passing over a telecommunications system is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication and is taken to continue to pass over the

system until it becomes accessible to the 'intended recipient' of the communication in section 5F and 'intended recipient' is defined as in section 5G as:

- individuals to whom the communication is addressed;
- if not an individual, the (corporate); or
- any person, or any employee or agent of the person, who has control over the telecommunications services to which the communication was sent.

Both section 5F and 5G provide a slightly different definition if the communication is sent by, or to, a range of agencies.

The *Telecommunications (Interception and Access) Act 1979* also defines the concept of accessing a stored communication to mean listening to, recording or reading a stored communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient in section 6AA. The distinction of knowledge means enforcement agencies are only regulated by the stored communications regime when they are acting covertly in accessing these communications. When acting overtly, existing access and compulsion powers of the enforcement agencies remain applicable.

The warrant regime

The *Telecommunications (Interception and Access) Act 1979* inserted a separate warrant regime for access to stored communications held by a telecommunications carrier. ASIO and enforcement agencies are treated differently within the regime.

ASIO can access stored communications in the same manner as it is able to intercept communications under a named person warrant in section 9(1a) of the *Telecommunications (Interception and Access) Act 1979*. This means the Attorney-General may issue warrants to ASIO to intercept communications where the communications are being used by a person who is 'reasonably suspected' of engaging in (or likely to engage in) activities prejudicial to security and the interception will, or is likely to, assist ASIO in its function of obtaining intelligence relevant to security.

In contrast, a stored communications warrant can be made available under a different and arguably lesser threshold, substantively set out in section 116 of the *Telecommunications (Interception and Access) Act 1979*, to an enforcement agency that is investigating a 'serious contravention'; or an offence which is punishable by a maximum period of imprisonment of at least three years, or a pecuniary penalty of at least 180 penalty units. Indeed this is not a trivial threshold, however the point to note is that the scope of offences defined as 'serious contraventions' prescribed in section 5E of the *Telecommunications (Interception and Access) Act 1979* is finite, but the decision to issue the warrant remains discretionary and based on the information made available to the authority issuing the warrant. Additionally, all enforcement agencies (criminal, civil and public revenue agencies) can obtain access to a stored communications warrant, whereas only law enforcement agencies (the Australian Federal Policy, the Australian Crime Commission and declared State and Territory law enforcement agencies) can obtain an interception warrant.

A stored communications warrant is only in force until it is first executed or 5 days after the day it is issued, whichever occurs first, pursuant to section 119(1) of the *Telecommunications (Interception and Access) Act 1979*.

Application of the legislative framework to email communications

Just as the *Telecommunications (Interception and Access) Act 1979* imposes a primary prohibition against interception, stored communications are also subject to a primary prohibition against access. It is an offence, subject to penalties of 2 years imprisonment and/or a significant monetary fine, for a person to access a stored communication or otherwise authorise access without the knowledge of the recipient or the sender of the communication under section 108.

'Access' is defined to mean listening to, reading or recording a communication (section 6AA). The threshold, like the other tests in the *Telecommunications (Interception and Access) Act 1979*, is whether or not the intended recipient had knowledge of the access (section 6AA).

Two initial observations are relevant:

- The Note to the prohibition against access in section 108 of the *Telecommunications (Interception and Access) Act 1979* specifically excludes accessing communications that are no longer passing over a telecommunications system from the intended recipient or from a device controlled by the intended. It appears this is intended to permit the forwarding of communications, and the recipient of that forwarded communication accessing that message (either email, SMS or MMS) and to permit law enforcement agencies to access communications which have already been received.
- The knowledge threshold in the definition of 'access' refers only to the knowledge of the intended recipient. However, the threshold in section 108 which states the prohibition against access refers to the knowledge of neither the intended recipient or the sender of the communication. One would think that the appropriate drafting would refer to a prohibition against access without the knowledge of either the sender or the recipient of a stored communication.

The conjunctive definition of a 'stored communication', as noted above, appears well-suited to describing an email communication. An email indeed becomes stored when it ceases passing over a telecommunications system, is held on equipment operated by and in the possession of a carrier (for example, the carrier's server or network equipment); and is unable to be accessed without the assistance of an employee of the carrier (excluding a person who is not a party to the communication – that is, the sender or a recipient).

This describes the normal functionality of an email communication. It leaves the server of an end user, which may be a company, and is carried by an ISP hosted on a carrier's network. That ISP of course may be the ISP of the host carrier (for example, BigPond on the Telstra Network). The electronic message is then carried to the ISP of the recipient's ISP located on the host's carrier network, to the server of the end user as delivered to the recipient.

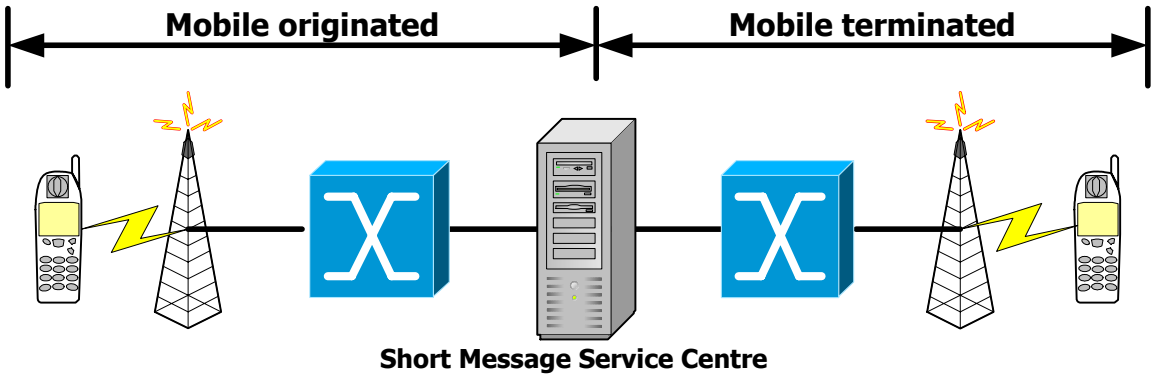
SMS/MMS communications

The definition of a stored communication, combined with the clarification of the 'passing over' concept (noted above), becomes problematic for SMS/MMS communications. The *Telecommunications (Interception and Access) Act 1979* has been constructed to describe the email scenario where a communication passes over a system and is then accessed by a recipient. The only other opportunity for access arise on the carrier side, by reference to the equipment that stores the email communication on the carrier's side.

In contrast, SMS/MMS communications are 'store and forward' messages. Unlike the direct transmission of an email from server to server via a network, SMS/MMS messages are

relayed by the sender's device indirectly to the recipient via a short message service centre or a (**SMSC**) or a mobile message service centre (**MMSC**). The SMS/MMS message is stored in the SMSC/MMSC which is essentially a processor with a server. The processor attempts to forward the message to the recipient device, often making several attempts over a defined period, such as 24 hours, before the delivery is successful. This is set out in Figure 4. It is informative to note that the when a mobile handset displays 'message sent' it simply means that the message has been received by the SMSC. The two parts of the SMS message, the mobile originated and mobile terminated are independent of each other.

Figure 4 – SMS as store and forward technology



Due to the enormous volume of messages transmitted to the SMSC/MMSC in any given period, messages are routinely deleted by carriers on a daily basis. As electronic files are never completely expunged, the retrieval of deleted messages is not impossible. However, it is extremely difficult and requires expensive technical processes to even locate an identifiable message. The relevance of this point is that the definitions of 'stored communication', 'passing over' and 'intended recipient' combine to require a communication to be accessible to the recipient and held on equipment operated by the carrier at its premises. In terms of the latter requirement, it is not impossible for a SMS/MMS to continue to be held on carrier equipment in some form.

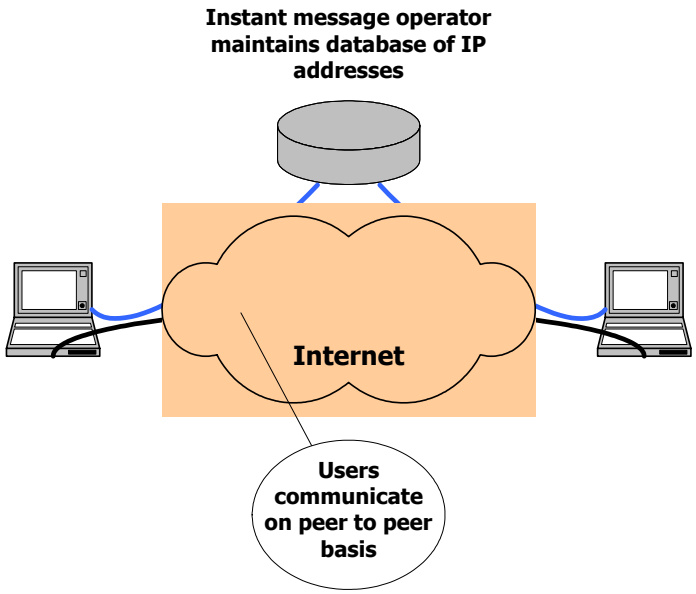
That is, an SMS is not a stored communication until the 'mobile terminated' element of the short message has occurred. However, the requirement for the communication to be accessible to the recipient (which defines the end of 'passing over a telecommunications system') is incapable of being satisfied. Once an end user deletes an SMS/MMS from their device, the message is incapable of being accessed by that person. The SMS is then 'passing over a telecommunications system' once more. In fact it remains passing over until it is deleted from the SMSC as the legislation is drafted. Importantly, a carrier has no way of knowing whether or not a message has been deleted from an end user's device. The consequence is that it is impossible for a carrier to know whether all of the limbs of the stored communication definition are satisfied at any point in time.

The practical implications for the carrier include making a judgment on whether or not access to a communication is subject to the stored communications warrant regime, or whether a search warrant is required pursuant to criminal legislation. This is highly problematic for the carrier, as warrants must be complied with. At the same time, a carrier risks criminal penalties for improper disclosure of communications. The inconsistencies require a judgment call that is impossible to satisfy in a practical sense.

Application of the legislative framework to instant messaging

The application of the *Telecommunications (Interception and Access) Act 1979* to instant messages is even more problematic. Instant message systems do not have any central storage facility. Instead, as set out Figure 5, messages are sent directly between users and the only need for a central system is to be able to identify the Internet Protocol address of the two parties to a message exchange.

Figure 5 – Peer to peer nature of instant messaging



When a person logs onto an instant message account such as Microsoft Messenger or Yahoo! Messenger, the central database checks to see if any of the person's contacts from their 'buddy list' are also signed into the system. Part of the process of signing in, allows the instant message system to identify the Internet Protocol address being used. Once the Internet Protocol addresses are known, each of the users of the instant message system can contact each other directly on a peer to peer basis. That is, there is no stored communication (but nor is there a standard form of communication which could easily be identified under a telecommunications interception warrant). As a practical matter, this issue is dealt with by operators of instant messaging systems contriving to ensure that the messages are stored centrally even though they would never have been 'passing over a telecommunications system' without the intervention of agencies.

Problems with location information

The *Telecommunications (Interception and Access) Act 1979* also imposes an obligation for carriers (and this includes carriage service providers) to provide communications metadata in near-real time and on a prospective basis. The impact on the privacy expectations of individuals is merely something to which the relevant bureaucrat should have regard when seeking the information. Unlike Europe or the US, no warrant is required for this data (Nicholls and Rowland 2008).

Operation of the law in practice

The introductory comments to this paper noted that operators who are subjected to the access and interception regime are being faced with the increasing difficulty of acting in the spirit, but not to the letter, of the law in matters of law enforcement. Whilst telecommunications is

not alone as an industry operating in a self-regulatory environment, our experience as legal and technical practitioners advising most of Australia's operators at some point has led to the conclusion that there are 3 key problems arising in the sector on matters of law enforcement.

First, some existing practices by law enforcement agencies are based on convention rather than the letter of the law. For example, we are frequently called to advise on warrants which have either expired, not been properly served, or are invalid for other fundamental reasons such as mis-naming the operator on whom is it purported to have been served. Frequently, warrants incorrectly cite the grounds on which access is being demanded. For example, section 182 of the *Telecommunications (interception and Access) Act 1979* is regularly stated as the basis on which access is being sought by a law enforcement agency. This is a legally incorrect ground for access. Section 182 is a provision which permits a person (in this case, a carrier) to disclose information to a law enforcement agency if that disclosure will assist in the enforcement of the criminal law and other matters. It operates as one of the exemptions to what would otherwise be an offence by the carrier to the prohibition against disclosure of communications information that is protected by law. It is not a provision which gives a law enforcement agency any rights at all to demand information, whether or not under a warrant.

Secondly, the gap between law enforcement agency appreciation for the technical limitations of their requests raises a raft of practical issues. We have seen stored communications warrants that have been issued covering periods of over 12 months, seeking all SMS messages sent and received by any person in a particular city, containing any or all key words listed in the warrant including (by way of illustration only) 'Arab', 'building', 'suitcase' and 'car'. Granted that certain combinations of words are likely to satisfy a reasonable suspicion test and may be no doubt critical to identifying and averting serious crimes, there still appears to be a limited understanding of the time and complexity involved for an operator to conduct a search of this nature and present it to a law enforcement agency in a meaningful way. As mentioned earlier, SMSC are purged of SMS messages daily to prevent the need for each operator to install vast server farms to store the billions of messages that are sent and received from their respective networks.

Thirdly, the level and multiple forms of regulation that permeate every aspect of the telecommunications operator's business – from its contracts with customers to the level of interconnection charges it can impose on other operators – means that the players have an acute awareness and sometimes heightened sensitivity to regulation that is often inconsistent and misunderstood. Take for example the by-product reactions of some law enforcement spokespeople during the now discredited Haneef proceedings. We saw some of the most senior law enforcement officers in Australia calling for identity checks to be undertaken before SIM cards were sold to consumers. As anyone who has a pre-paid mobile service will attest, a system of pre-paid identity verification has operated in Australia for years, as well as an existing statutory requirement for all operators to provide information about phone numbers and their subscribers to an integrated public number database (**IPND**). Our experience is that telecommunications operators understand that the nature of the industry requires a form and level of regulation not seen in other sectors, but inconsistent approaches to regulation and continually being made 'the fall guys' for the sake of a media grab does nothing to progress the carrier-law enforcement agency relationship.

The following examples provide a flavour of the issues that arise for carriers in their access and interception compliance obligations on an almost daily basis.

Operators receiving stored communications warrants for SMS

Despite the analysis presented above, various law enforcement agencies have served warrants on mobile operators for the contents of SMS. The practical result of such a warrant is that the operator provides the law enforcement agency with the communication content of all SMS for any identified target individual. That is, personnel within the mobile operator's business determine that it is more appropriate to respond to a warrant which may be incorrectly served than it is to decline to fulfil the warrant on the basis that to do so could lead to that individual serving a prison term of up to two years.

Operators receiving warrants for instant messaging

As set out above, instant messages are peer to peer communications which are not stored (other than on the computers of the users). Nevertheless, operators of instant messaging systems do receive requests for assistance and the Australian branches of the multinational corporations which provide such services may receive warrants. The practical result of the warrant being served is that the operator of the instant messaging system routes messages specifically to a facility so that the messages can be recorded and sent on to the requesting law enforcement agency.

State bodies seeking assistance in contravention of Commonwealth statute

Certain State-based statutory bodies have power under their establishing legislation to demand the production of documents and materials. Despite the fact that there is an obligation not to disclose material of the form of interception related information under the *Telecommunications (Interception and Access) Act 1979*, the normal outcome of such requests is that the material is provided to the State body — despite the fact that such inconsistencies should mean that Commonwealth law 'trumps' State law by virtue of the Constitution.

Requests for information or action without a warrant

It is common practice for bodies such as LEAs and public prosecution entities to issue requests for information or action by operators in the absence of a warrant, citing provisions such as section 182 of the *Telecommunications (Interception and Access) Act 1979* as the head of power. As mentioned previously, this is an exemptions provision and not a standalone head of power. In some cases when the validity of those requests is questioned on this basis, we know of operators that have had section 313 of the *Telecommunications Act* quoted back to them. Section 313 is an 'umbrella' obligation that requires a carrier or carriage service provider to give law enforcement agencies 'such help as is reasonably necessary' to, among other things, safeguard national security. The purposive approach to statutory interpretation appears to have been disregarded by reliance on such a broad power rather than specific provisions of the *Telecommunications (Interception and Access) Act 1979*.

It is ironic that the Australian Law Reform Commission's 'Privacy Review' (ALRC 2008) reports that Simon Bronitt and his co-researchers identified a 'loophole' in the Telecommunications (Interception and Access) Act 1979 in their submission to the review (Bronitt, Stellios et al. 2007). This loophole permits access to a stored communication with the permission of only one of the parties to that communication. This omission, on which the ALRC noted 'that the circumstances in which communications can be intercepted is an issue that is outside the scope of' its inquiry (ALRC 2008 p 2486), is already being used by State law enforcement agencies.

Location based data

As a practical matter, mobile operators in Australia have the capacity to deliver call associated data on a prospective basis. This means that the effect of the 2007 legislative amendments is simply a mechanism to require operators to deliver the communications metadata. However, this does not mean that law enforcement agencies are able to locate targets with any great precision. Location based services use multiple techniques in order to determine the location of a customer and the legislative package does not, making a reasonable assumption about the nature of 'telecommunications data', impose an obligation on carriers to provide a location based service. Rather, it requires that cell site information is provided.

Carriers typically provide more accurate location based information in response to particular safety of life situations. When there is a potential suicide, for example, a carrier may assist authorities by triangulating the position of a person based on a handset in operation. This is not a standard location based service and requires significant engineering effort. Further, it is not the type of information that would lend itself to prospective data delivery.

The increasing use of location based services (Bowen and Martin 2007) means that there should be no assumption that the location based information associated with such services would not fall into the definition of 'telecommunications data' at some point in the future. The major reason for the absence of a definition of telecommunications data in the legislation is that the term was expected to evolve with technology over time. In particular, the development of standards for the presentation of location information (Adams, Ashwell et al. 2003) potentially herald this. In turn, this leads to the biggest issue arising from the regulatory changes which faces mobile operators in Australia. As has been pointed out in the past, mobile operators have been more than willing to ensure that they comply with their obligations in meeting the legislative regime and in many cases deliver more than is required under the poorly drafted legislation which imposes broad duties of assistance (Nicholls and Rowland 2007). The likelihood is that the criminal enforcement agencies and ASIO will decide that telecommunications data has a larger meaning than merely call associated data. As this changes over time, there is no provision for a review of the undefined term.

The problem is compounded by the fact that law enforcement agencies represent an epistemic community. That is, the agencies discuss issues with each other and created a consensus view which relates to all of the agencies' needs. As a result, the meaning of terms such as 'telecommunications data' will evolve more rapidly than would be determined by any one of the agencies. In effect, the legislative framework under the *Telecommunications (Interception and Access) Act* 1979 provides an environment where the metadata delivered is determined by the agencies which require the data at their sole discretion. Whereas there is typically agency design in the way that communications content and metadata is delivered (Nylund 2000), the absence of external review, even on a cursory basis, does not represent regulatory best practice. Indeed, as the legislation gives the Attorney-General the power to determine the method of delivery of communications content consistent with international standards (section 189), it is odd that the delivery of communications metadata is left entirely in the hands of the agencies.

To some extent, there is already evidence of this in the delivery of communications content. The 2008 amendments to the *Telecommunications (Interception and Access) Act* 1979 have significant effect (Rowland and Alderson 2008):

> The proposed amendments mean that a named person warrant, issued in respect of devices, will authorise interception of communications on any telecommunications device that the person uses, or is likely to use to the extent that they are known at the time of

> applying for the warrant. ASIO and other law enforcement officers would be able to intercept all communications made by means of any telecommunications device used by a named person of interest, rather than first identifying in the warrant all of the particular telecommunication devices to be intercepted.

The legislative changes are also generally more profound than simply changing the obligations for supply of communications metadata. All of the obligations associated with the provision of communications content and communications metadata have been moved from the *Telecommunications Act* 1997 to the *Telecommunications (Interception and Access) Act* 1979. The effect of this change is to remove (except by limited and partial reference) all of the objects of the *Telecommunications Act* 1997. This changes the regulatory paradigm for interactions between carriers and law enforcement agencies from one based on self-regulation and increasing diversity of services to one where the legislation has no stated objects. There is also a significant widening of the scope of the legislation. The previous regime imposed an obligation for interception and assistance on carriers and carriage service providers with distinctions between the two. The *Telecommunications (Interception and Access) Act* 1979 does not draw such a distinction and, indeed, conflates the two concepts into the single defined term 'carrier' in section 5.

Legislative amendments

It seems to us that the next round of amendments to the Telecommunications (Interception and Access) Act 1979 (and we fear that the annual amendments will continue for some time) should recognise that there are store and forward services where the 'forward' element is not under the control of the user, such as SMS. It should also recognise that peer to peer instant messaging requires intervention which routes the communications in a different way than usual in order to provide interception or access (and that the legislation is required to be clear on this point). That is, rather than placing operators in the position where individuals risk their liberty to meet the spirit of the law, the law should provide a bright line to ensure that the distinction between lawful interception and access as compared with individual privacy expectations is clear.

Summary and some conclusions

Telecommunications operators in Australia are being increasingly compelled to compromise their strict obligations under the law with a desire to be viewed as co-operative rather than obstructionist with LEAs. Our view is that too many 'commercial calls' and 'one-off relationship decisions' are made on issues of national security obligations that should be clearly articulated in legislation and in practice. This is an untenable situation and needs to be urgently addressed by a more thorough and thoughtful application of the law by all parties. Regulation of telecommunications for national security purposes is rightly viewed as serious. It should be applied seriously and with the strictest and most robust legal standards.

The social implications of our conclusions are stark. There is an individual expectation that calls will not be intercepted and that communications will not be accessed because, as a matter of law, there is a strict prohibition on such interference. In practice, this strict prohibition has been compromised under the banner of commercial expediency and an over-zealous support of the spirit (but not the letter) of a legislative regime which seeks to provide protections against terrorism and other crimes. If the results of this enthusiasm are a reflection of the inadequacy of parliamentary drafting, then the appropriate course is to redraft the legislation.

BIBLIOGRAPHY

Adams, P. M., W. Ashwell, et al. (2003). 'Location-based services — an overview of the standards.' *BT Technology Journal* **21**(1): 34–43.

ALRC (2008). For Your Information: ALRC Report on Australian Privacy Law and Practice. Sydney, ALRC. **3**.

Bawa, N. (2006). The Regulation of the Interception of Communications and Provision of Communication Related Information Act. *Telecommunications Law in South Africa*. L. Thornton, Y. Carrim, P. Mtshaulana and P. Reyburn. Johannesburg, STE Publishers.

Bellovin, S., M. Blaze, et al. (2006). Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP. Washington, Information Technology Association of America.

Bowen, C. L. and T. L. Martin (2007). A Survey of Location Privacy and an Approach for Solitary Users. *40th Annual Hawaii International Conference on System Sciences*. Hawaii, IEEE.

Branch, P. A. (2003). Lawful Interception of the Internet. Melbourne, Centre for Advanced Internet Architectures, Swinburne University of Technology.

Bronitt, S. and J. Stellios (2006). 'Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?' *Prometheus* **24**(4): 413–428.

Bronitt, S., J. Stellios, et al. (2007). Submission PR213 to the Australian Law Reform Commission Privacy Review. Canberra, ALRC.

Del Bianco, M. C. (2006). 'Voices Past: The Present and Future of VoIP Regulation.' *CommLaw Conspectus* **14**: 365–401.

Drinan, H., N. Fontaine, et al. (2005). 'News Briefs.' *Security & Privacy Magazine, IEEE* **3**(6): 7–8.

ETSI (2007). Lawful Interception (LI): Handover interface for the lawful interception of telecommunications traffic. ETSI ES 201 671 V3.1.1 (2007-05). Sophia Antipolis Cedex — FRANCE, European Telecommunications Standard Institute.

Fonknechten, D., B. Ghribi, et al. (2004). 'Service Aware Intelligent GGSN.' *Alcatel Telecommunications Review* **1st Quarter 2004**: 2–10.

Gidari, A. (2006). 'Designing the Right Wiretap Solution: Setting Standards under CALEA.' **IEEE Security and Privacy**(May/June 2006): 29–36.

Gratzer, V., D. Naccache, et al. (2006). *Law enforcement, forensics and mobile communications*. Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on.

Holland, B. (2004). 'Overtaking privacy in the telecommunications transit lane.' *Privacy Law and Policy Reporter* **10**.

Landau, S. (2005). 'Security, Wiretapping and the Internet.' *Security and Privacy Magazine, IEEE*(December 2005): 26–33.

Miettinen, K. (1999). Lawful Interception in GPRS/UMTS Network. Helsinki, University of Helsinki.

Milanovic, A., S. Srbljic, et al. (2003). *Methods for lawful interception in IP telephony networks based on H.323*. EUROCON 2003. Computer as a Tool. The IEEE Region 8.

Milanovic, A., S. Srbljic, et al. (2003). *Distributed system for lawful interception in VoIP networks*. EUROCON 2003. Computer as a Tool. The IEEE Region 8.

Miller, H. G., H. D. Levine, et al. (2005). 'Welcome to convergence: surviving the next platform change [Internet protocol].' *IT Professional* **7**(3): 18–25.

Nicholls, R. and M. Rowland (2007). Message in a bottle: Stored communications interception as practised in Australia. *From Dataveillance to Überveillance and the Realpolitik of the Transparent Society: The Second Workshop on the Social Implications of National Security*. M. Michael and K. Michael. Wollongong, Wollongong University.

Nicholls, R. and M. Rowland (2008). Regulating the use of telecommunications location data by Australian law enforcement agencies. *Third Workshop on Social Implications of National Security* K. Michael and M. G. Michael. Canberra, University of Wollongong**:** 115–124.

Nolin, C. A. (2006). 'Telecommunications as a Weapon in the War of Modern Organized Crime.' *CommLaw Conspectus* **15**(Fall 2006): 231.

Nylund, J. J. (2000). 'Fire With Fire: How the FBI Set Technical Standards for the Telecommunications Industry under CALEA.' *Commlaw Conspectus* **8**: 329–348.

Open Mobile Alliance (2005). Push to talk over Cellular (PoC) — Architecture. La Jolla, Open Mobile Alliance.

Rowland, M. and S. Alderson (2008). 'New telecommunications interception and access proposals: the first or last of many?' *Communications Law and Policy Bulletin*(May 2008).

Schwaderer, C. (2007). Lawful surveillance systems: Enforcing justice while protecting individual privacy. *CompactPCI and AdvancedTCA Systems*.

Street, M. D. (2003). *Interoperability and international operation: an introduction to end to end mobile security*. Secure GSM and Beyond: End to End Security for Mobile Communications, IEE Seminar on (Digest No. 2003/10059).

Williams, N. and J. Ly (2004). Securing Public Instant Messaging (IM) At Work. Melbourne, Centre for Advanced Internet Architectures, Swinburne University of Technology.