Federal Criminal Law and Mobile Telecommunications Devices

Implications for Law Enforcement through Trends and Issues

Aaron Read

5479 wds

A Hypothetical

A nondescript man walks into a Rundle Mall café and takes out his mobile phone. Seen by patrons – unaware that he is a suspect of the Australian Federal Police in an ongoing terrorism investigation – he plays with the device for some time, then makes a phone call apparently confirming a number of details. He then makes another call threatening 'the event' will take place that day unless demands are met, then leaves the store. The patrons of the store are unaware of a number of things.

They are unaware that the man was actually posting about suicide attacks on a terrorist website;[1] *that the first phone call was to confirm a large amount of data in relation to a proposed terrorist attack later that day; and that the second was a threat made to the government regarding the target. All of these acts have the obvious potential to breach a seemingly endless stream of offences under Federal Criminal law: and would be of high relevance and important ones from the perspective of the AFP at that.*

[1] See below at 5.5.

Most importantly in this hypothetical example is that most of them at least are unaware that the device the man is using is not a mobile phone at all. In fact it is a modern Windows Mobile Personal Data Assistant, or PDA (also known as Pocket PC).[2] *This device is not using the traditional mobile phone networks (such as the GSM or CDMA networks) at all, but is connecting over personal computing wireless standards to a wireless 'hotspot', or free internet access point provided by the café for customers.*[3] *Further, all communications were effected via a VOIP program with built in encryption.*[4]

1. An Explanation

1.1. The purpose of this story is to attempt to give some idea of the current status of the evolution of mobile telecommunications technology, and foreshadow some of the likely problems that such technology will present for law enforcement.

1.2. In 1997 Gerard Walsh (ex-deputy director of ASIO), in the highly controversial and discussed Review of Policy relating to Encryption Technologies,[5] speaking on the issue of this impact stated that it 'remains fairly negligible, though the problem is only as far away as tomorrow'.[6] At that time, mobile phones were markedly simple with technology such as GSM and SMS still being relatively new.[7] Also at that time, the early

[2] See Microsoft Windows Mobile website: <http://www.microsoft.com/windowsmobile/default.mspx>.
[3] See, eg, Internode, *News and Media: Adelaide to Boost Free Wireless Web Reach by 250%* (2007) <http://www.internode.on.net/about/news/20060808-citylan.htm> at 1 June 2007. See also Internode Wireless Hotspot information site: <https://hotspot.internode.on.net/> . Also below n 12 at 15.
[4] See, eg, Skype for Pocket PCs: <http://www.skype.com/download/skype/mobile/> at 14 May 2001.
[5] Commonwealth, Gerard Walsh, *Review of Policy relating to Encryption Technologies* (1997).
[6] Ibid, [5.1.8].
[7] At the time of the research conducted for the Walsh report (1996), SMS was 5 years old: GSM Favourites, *Introduction to SMS* <http://www.gsmfavorites.com/documents/sms/introduction/> at 22 May 2007.

predecessors of today's Windows Mobile 'Smartphones' (PDA devices with mobile telephone functionality) – such as the Casio Cassiopeia were extremely basic – with original examples providing only primitive internet (no wireless)[8] connectivity – and more closely resembling laptops than the handheld units of today.[9]

1.3. A decade later, the differences between mobile phones and Windows Mobile (and some other) PDA's have become blurred and in many ways mere technicalities with the introduction of the newer 'Smartphones', such as the popular O2 XDA series,[10] as well as the increasing trend for mobile phones to mimic and implement the features of these devices.[11]

1.4. This trend has not gone unnoticed by the Federal Government, who in a recent review of content delivery legislation produced charts and diagrams illustrating the convergence occurring from both ends of the spectrum in terms of both connectivity protocols and general features.[12] As stated in that report, speculation as to the exact path the technology may take in future incarnations is rife in all directions, but 'whichever view proves correct, the increasing capabilities of devices suggest that

[8] HPC Factor: *CESDC0033 – Windows CE 2.0 and Ethernet / Wireless Network Connectivity* <http://www.hpcfactor.com/support/cesd/c/0033.asp> at 22 May 2007.
[9] See, eg, HPC Factor: *The History of Microsoft Windows CE* <http://www.hpcfactor.com/support/windowsce/> at 22 May 2007.
[10] See, eg, O2 XDA Website <http://www.seeo2.com/> at 22 May 2007.
[11] Most major manufacturers such as Motorola, Nokia and LG market increasingly popular examples of such devices, which can be found almost exclusively at all leading retailers.
[12] Commonwealth, Department of Communications, Information Technology and the Arts, *Review of the Regulation of Content Delivered over Convergent Devices* (2006). See especially p 17.

consumers will soon be able to access a wide range of rich audiovisual content on the move'.[13]

2. Formal Introduction

2.1. From the hypothetical it can be seen that the topic of telecommunications is extremely broad – there is a seemingly endless supply of literature of all of the issues, which are many times more what any paper of reasonable length can hope to cover.

2.2. The purpose of this paper is to examine the law enforcement impact of what might be called the "Federal Law of the Mobile Phone" – or perhaps more sensibly the "Federal Law of the Mobile Telecommunications Device" – through a series of issues, past and present, in order to see if the relevant laws will need to change. As will be seen, this may not be as simple as mere technical changes, but rather much deeper changes to the ways of thinking about the issues. Once this is done – and only once this is done – can a relevant context be created for useful discussion of recommendations.

3. The Model Criminal Code

3.1. The logical starting point within the relevant legislation is a series of provisions within the *Commonwealth Criminal Code*,[14] specifically Part 10.6: 'Telecommunications Services'.[15]

[13] Ibid, 16.
[14] *Criminal Code Act 1995* (Cth).

3.2. The Part is separated into three divisions: Division 473 dealing with preliminary definitional issues; Division 474 containing the offences themselves; and Division 475 dealing with miscellaneous provisions including the geographical coverage of the part.

3.3. Under Division 473, 'Extended Jurisdiction A' is applied, which under s 15.1 of the Act applies where the conduct or result of the offence occurs wholly or partly within Australia, *or* on board an Australian aircraft or ship, *or* where at the time of the offence the person accused was an Australian citizen or body incorporated under Australian law, *or* an ancillary offence occurring wholly outside Australia with the conduct or result comprising the primary offence being intended to occur inside Australia or aboard an Australian ship or aircraft.

3.3.1. The only limitation is the 'no foreign offence defence' provided for the jurisdictional category contained in subs (2)-(5). It has been suggested that this is insufficient.[16] The multi-jurisdictional nature of telecommunications, and their ability to be routed around or through a number of jurisdictions means that extraterritorial provision may be required.

3.3.2. In light of the inherently required international co-operation in such cases, one must query whether such provision would aid Australia. The situation put forward by the AFP in support of the

[15] Of course, the computer offences contained in Part 10.7 also have the potential to be relevant.
[16] Commonwealth, Information and Security Law Division Attorney General's Department per Peter Ford, *Telecommunications Interception Policy Review* (1999) at [7.1.12].

proposition involved communications merely passing through Australia.[17] It seems likely that most offences or potential conduct occurring or to occur inside Australia would involve communication passing at one point within Australia, and as such covered.

3.3.3. However, given that many of the issues are transnational in nature, the benefits that would flow from international co-operation are hard to deny. Continued progress may be dependent upon such,[18] and to that extent it seems wise to expand the geographical jurisdiction, if only for the purposes of interception, which is discussed below.

3.4. Division 474 is further usefully divided into 3 subdivisions: Dishonesty with respect to carriage services; Interference with Telecommunications; and Offences related to the use of telecommunications. It is with the second of these that our exploration begins.

3.5. The provisions contained within Subdivision B can be viewed as arising directly from the earliest issues arising from the development of the mobile phone: mobile phone theft and fraud. These crimes arise from the traditional billable mobile phone communications. A brief look at the history of the technology is useful.

3.6. Early high-volume cellular phones were Analogue and communicated with the network on an unencrypted basis. In order to identify the phone (and thus the customer to bill), the phone would broadcast an ESN/MIN

[17] Ibid, [7.1.10].
[18] Ibid, [7.1.17].

combination that was burned into a chip on the phone. This transmitted the manufacturer/serial number of the unit, and the ten digit area code and phone number respectively.[19] In addition to theft, fraud was committed in both traditional ways,[20] as well as via the use of advanced technology.[21] Devices were made to scan the output of such phones in order to obtain the ESN/MIN codes in order to modify existing phones – a process called 'cloning'.[22] A final problem was the creation of a limited number of illegal 'lifetime phones' – which had completely programmable ESN/MIN codes.[23]

3.7. The later digital GSM phones resolved some of these difficulties via handsets having an IMEI that identified no more than the handset, and all of the billing and number identifying information being contained on SIM cards that are inserted into the phone. Similar but technically different issues arise on modifying SIM cards and the possession and use of blank SIM cards for similar purposes.

3.8. Both Legal and Commercial responses ensued, because of the large cost to organisations and the community of the crimes.

3.9. The legal response to this kind of crime can be seen in a number of sections:

[19] Russel G. Smith, 'Preventing Mobile Telephone Crime' (1996) 54 *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*, 1.
[20] Australian Federal Police, '*Mobile phone crime brings new challenges in emerging trends for law enforcement*' (1998) Platypus Magazine, [1].
[21] Or sometimes not so advanced. Overseas, by changing the ESN/MIN fast enough, one could make short calls for free. Movement to pre-call validation resolved this issue: Above n 19, 4.
[22] For interesting motivators, see above n 19.
[23] Ibid, 4.

3.9.1. 474.4 deals with 'interception devices', defined under 473.1 as being a device capable of and being designed for intercepting a communication passing over a telecommunications system. Prohibited is the manufacture, advertisement or display for sale, sale of or possession of an apparatus or device fitting that description, punishable by five years imprisonment. Defences are provided in subs (2) and (3) for people acting within their duties under Interception legislation or for regulations pursuant – effectively excluding lawful conduct. Because the offence is defined by reference to communications passing over and not to *any* specific device, this section is effectively future-proofed against new technology.

3.9.2. 474.5 has potential application to the issue of cloning, prohibiting causing the delivery of communications to a person or service not intended or for which consent was not given.

3.9.3. 474.7 deals with the substantive issue of modification of 'telecommunications device identifiers', defined under 473.1 as an electronic identifier of a mobile telecommunications device,[24] which is installed by the manufacturer and capable of being used to distinguish the device from others. A note in the Act expressly makes reference to the IMEI number of modern digital GSM phones – the definition would be equally applicable to the ESN component of the

[24] Defined simply as a customer device that is used or capable of being used in connection with a public mobile telecommunications service.

old analogue phones. The section prohibits modification or interference with such an identifier without consent of the manufacturer, with defences for the manufacturer themselves and employees or agents of the manufacturer acting on behalf of them. This section provides punishment as 2 years imprisonment.

3.9.4. 474.8 and 474.9 act as satellite provisions to 474.7. 474.8 makes it an offence (excluding attempts),[25] to have possession or control of data or a device with intent to modify as in 474.7, regardless of whether actually committing the offence is impossible.[26] Exclusions for law enforcement officers and manufacturers and employees apply.[27] Penalty is 2 years imprisonment. 474.9 is in like terms with like defences,[28] but makes it an offence to produce, supply or obtain data with the intention that the person or any other person will use for the purpose of an offence against 474.7. Penalty is again 2 years imprisonment.

3.9.5. With 474.11 and 474.12 replicating the possession or control and producing, supplying or obtaining data or device satellites, 474.10 creates a similar scheme to that of 474.7 except in this case dealing with 'subscription specific secure data' (SSSD).[29] There are two provisions, subs (1) and (2), the former prohibiting the copy of SSSD

[25] 474.8(3).
[26] 474.8(2).
[27] As noted in the Act, a defendant bears an onus of proving such a matter.
[28] *Criminal Code* ss 474.9(4), (5).
[29] Defined under the Act as data identifying an account (existing or future), and allowing a device in which it is installed access to the network to which the account relates.

with the intention it will be copied to something that is an account identifier or once copied will be an account identifier,[30] the latter ensuring there is no escape from the first by repeating it but instead of referring to the copying of data referring to the use of copied data. This section is said to apply regardless of whether the person knows where the data came from.

3.10. All of the sections and definitions are phrased in technology neutral terms, so as to ensure that any future technology will still be covered by the provisions. One difficulty that may be faced is the lack of a universal unique and indelible identifier in future technology.[31] While Smartphones connecting to GSM or 3G or other traditional networks all utilise IMEI numbers, standalone PDA's (or Smartphones while connecting to wireless networks) do not broadcast any such IMEI number. While all wireless devices do have a somewhat unique identifier: the MAC address. Currently, all devices utilising computer networks to access telecommunications systems require a MAC address. However, as has been noted by Electronic Frontiers Australia (EFA), the MAC address of a device cannot be changed physically easily at all, but software can be relatively simply used to create the impression that it has been changed.[32]

[30] The 'once copied' text is includes blank SIM cards, (or presumably blank EEPROM chips): Explanatory Memorandum, Crimes Legislation Amendments (Telecommunications Offences and Other Measures) Bill 2004 (Cth), 16.
[31] Anthony S. Blunn: Commonwealth, Attorney General's Department: Public Affairs Unit, *'Report of the review of the regulation of access to Communications*' (2005), 46.
[32] EFA, *'Submission to the Senate Legal and Constitutional Legislation Committee "Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006'* (2006) <http://www.efa.org.au/Publish/efasubm-slclc-tiabill-2006.html> at May 23 2007.

For technical reasons, while the provisions of 474.7 are potentially applicable, law enforcement prospects may be dubious. As will be seen, this will become a theme for such devices.

3.11. Finally, Under the Pre-Paid Identity checks Determination,[33] certain identification information must be obtained and verified before any pre-paid services are activated.

3.12. Before moving to the next topic, it is worth looking at the commercial action taken in response to this problem. Each of the major telecommunications bodies have a number of databases from which they share information to combat different parts of these more general issues.

3.13. A key database of this variety is the IMEI blocking feature, which was developed as a joint enterprise between the Australian Mobile Telecommunications Association, State and Territory Police forces, and the major telecommunications carriers.[34] Persons can check if their phone is on the stolen list by checking their IMEI against this database at the AMTA site.[35] Individual telecommunications carriers also have technical arrangements to detect 'cloned' phones, or those sharing IMEIs and operating on the network at the same time or at similar and impossible times. Such cross-listing is required to avoid the previously difficult problem of 'rebirthing' on new networks. While it may be better for an

[33] *Telecommunications (Service Provider - Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000* (Cth).
[34] AMTA, *'Mind Your Mobile'* <http://www.amta.org.au/default.asp?Page=132> at May 22 2007.
[35] AMTA, *'Check the Status of Your Handset'* <http://www.amta.org.au/default.asp?Page=405> at May 22 2007.

entirely government funded and operated facility to be in place, there is little to suggest that the individual carriers are not meeting their requirements.

3.14. As an example, Optus uses a system called "Focus". When a stolen or lost IMEI is detected, a network announcement is issued stating as such and non-emergency call operation is not allowed.[36] Where two or more instances of the same IMEI are detected, they through a special department called the Law Enforcement Liason Unit will contact police and initiate procedures in an attempt to resolve the matter. A high-ranking Optus technical support officer has stated that in their many years working in the area, they have only witnessed one instance of such conflict, which turned out to be a manufacturer fault with no foul play involved. However, whether actual figures are withheld to protect their public image may be a consideration. The literature does however suggest that for digital GSM phones, SIM cards and not IMEI issues are more prevalent.

3.15. The author does note that IMEI changing services appear to be relatively easy to find online, and lack of IMEI conflicts may simply be a result of criminals or other users simply 'getting lucky' with an unused IMEI. Telecommunications organisations did not expressly deny this was possible.[37] While sources like these may lead to the belief carriers are

[36] Interview with Anonymous Technical Support Officer, - personal details withheld for anonymity reasons, Optus (Telephone interview, 18th May 2007).
[37] Ibid.

doing all they can, there seems to be evidence to support the contention that they act only where legally obligated or for profit. An interview the author conducted with a police officer who had had recent dealings with a major carrier's law liason unit with respect to a lost mobile phone supports this contention. Under Privacy laws, the owner of the phone was not allowed to be identified via the IMEI, so reliance had to be placed on the carrier to resolve the issue. After two weeks and several attempts to get them to inform the owner of the rather expensive telephone, police lost property policy resulted in the phone being destroyed.[38]

4. The Critical Link: Anonymous Phones and Criminal Activity

4.1. The utility of phones to criminal enterprise – especially where there is no way to trace the criminal to the phone – is obvious.[39]

4.2. A brief story that brings all these issues together and sets the scene for the interception issues is the American story of 'Cellmate'.[40] Here, police in co-operation with a carrier (providing the tech and free air time for the purposes of a sting operation) set up an underground illegal phone services company that provided illegal phone services to criminals. This was conducted in the knowledge that illegal activities using the phones could thwart traditional wire-tapping techniques. After providing many criminals with phones and gathering evidence, they were duly rounded up

[38] Interview with Police Constable – identity and date withheld for privacy reasons.
[39] Above n 19, 5-6.
[40] Above n 20 at [2]-[6].

and charged with not only the phone offences but other offences – with the detailed call records proving useful in the detection and proof of other offences. A notable example here was the ensuing Naval Criminal Investigation Service (NCIS) inquiries into sailors using the phones to make bomb threats to get days off of work. Such hoax calls (or indeed real threats) would constitute offences under the *Criminal Code*.[41]

5. An Emerging Law of Criminal Communications?

5.1. Communication that is in itself criminal, or communication conducted in aid of criminal offences is recognised by legislation in the third subdivision of Division 474 of the *Criminal Code*.

5.2. Warranting comment is the targeting of two specific sets of provisions, namely those relating to child abuse or child pornography and the suicide materials provisions. (The latter given recent media attention because of euthanasia activist Nitschke.) Despite claims that the laws were poorly conceived,[42] and despite the obvious implications of free speech, the general structure shared by the two are worthy of comment.

5.3. A person is guilty under the key provisions of the respective categories if they: (1) use a carriage service (2) to access, cause to be transmitted, make available or publish or otherwise distribute, (3) material, and (4) the material is of the kind specified and defined under the respective section. Intention is the requirement for (2), and recklessness is acceptable for (4)

[41] See *Criminal Code* ss 474.15, 474.16, 474.17.
[42] Kim Wheatley, 'Nitschke admits to secret death code', *The Advertiser* (South Australia), May 2 2007, 12.

in the case of child abuse or pornography material, with intention to directly or indirectly incite or to be used by another to counsel or incite committing or attempting to commit suicide or a method thereof being required for (4) for suicide material.[43] Penalties of up to 10 years apply.

5.4. They are worthy of note because of their format: that they specifically target types of material or communications, that they are technology neutral (one need merely involve transmission via a carriage service), and consequently extremely broad. Defences are available on limited grounds for all of these offences and are provided for in the relevant sections and accompanying sections.

5.5. Perhaps more noteworthy are the corresponding preparatory offences: the possession, control, supply or obtaining with intent provisions.[44] Guilt is established on those grounds where intention that the material is to be used in commission of the carriage service offences can be established, regardless of impossibility.[45] The creative leeway thus provided for in these offences is rather staggering. In the words of an explanatory memorandum,[46] 'As an example, the offence would apply to the possession or production of paper leaflets providing instruction on a particular method of suicide, provided the person engaging in this conduct intended that the leaflets also be made available on the internet

[43] See *Criminal Code* ss 474.19; 474.22; 474.29A.
[44] Ibid, ss 474.20; 474.23; 474.29B.
[45] Ibid.
[46] Explanatory Memorandum, Criminal Code Amendment (Suicide Related Material Offences) Bill 2005 (Cth) 4.

for the purpose that it be used by another to commit suicide'. Given the defences are limited to use for the purposes of public discussion about law reform or advocate law reform of the law relating to euthanasia or suicide and only then provided that the person does not nevertheless intend to incite or promote or be used for suicide or a type of suicide,[47] and that suicide bombing is a form of suicide (actively promoted by terrorists, the room for creativity is obviated.

5.6. The types of specific crimes that may be committed has thus expanded, but so too have the advantages of telecommunications in criminal activity has likewise expanded. Against this backdrop, the seriousness of trends and issues with respect to the effect of technology on law enforcement can be examined.

6. Anonymity and Freedom in Telecommunications and the Difficulties Faced by Law Enforcement

6.1. It almost goes without saying that for police to be able to eavesdrop on criminal conversation – either to gain evidence of offences being committed by means of the conversation itself, or as use merely as an investigative/evidence-gaining tool – represents a substantial power and asset and advantage of police.[48] The advent of telecommunications provided this advantage – but the increasing anonymity, mobility, and security of telecommunications threatens that advantage.

[47] *Criminal Code* ss 474.29A(3), (4).
[48] Above n 16.

6.2. In addition to the flood of other data, there have been a number of other key legislative reforms and three reports in particular which help draw out the remainder of the issues. The legislation which the reforms have surrounded includes the *Telecommunications Act*,[49] (henceforth TA) the *Telecommunications (Interception and Access) Act* (known until recent amendment in 2006 as the *Telecommunications (Interception) Act*,[50] (henceforth TIA) and the *Cybercrime Act*.[51] The four reports with the most relevance are commonly referred to as the 1997 report of Gerard Walsh (encryption),[52] 1999 report of Peter Ford (interception policy review),[53] the 2003 report of Tom Sherman (interception policy review),[54] and the 2005 report of Anthony Blunn (regulation of access to communications).[55]

6.3. Similar issues arise throughout all of the literature, however some perspective can be gained from the comment of Blunn that the increasing challenges posed by emerging technologies and compounded by industry considerations involve three elements: Identification, Data Capture, and Understanding.[56]

[49] *Telecommunications Act 1997* (Cth).
[50] *Telecommunications (Interception and Access) Act 1979* (Cth).
[51] *Cybercrime Act 2001* (Cth).
[52] Above n 5.
[53] Above n 16.
[54] Commonwealth, Tom Sherman, *Report of review of named person warrants and other matters* (2003).
[55] Above n 31.
[56] Above n 31, [3.1.2].

7. Identification and Interception

7.1. These two issues are related by necessity: one cannot intercept something that has not been identified. Interception is useful to the police not only for data gathered, but because it is generally much cheaper and safer than human intelligence and investigation.

7.2. The ways in which the different physical hardware can be identified are in part the consideration of the legislative provisions and ideas already discussed above at 3.9.3 and 3.10. The subject of much of the jurisprudence on this issue, however, focuses on the Interception provisions of the TIA.

7.3. As outlined in more detail up until 2003, the Sherman Report contains a good history of the TIA:[57]

7.4. 1960: Regulation of Telecommunications Interception (TI) in Australia began with the *Telephonic Communications (Interception) Act 1960* which made it an offence to intercept telecommunications, with the exceptions of technical reasons (including nuisance calls) and under warrant from the Attorney General to ASIO for national security purposes – with minor exceptions for grants by the Director-General of security in emergencies.

7.4.1. 1979: The *TIA 1979* was introduced and extended exceptions to narcotics offences under the *Customs Act 1901*, as well as beyond

[57] Above n 54, 7.

voice communications to other telecommunications such as data. Since the Internet, such definition is essential.

7.4.2. 1987: Amending legislation extended warrants coverage to serious crimes in a similar fashion to what is in existence now defined under section 5D of the *TIA*.[58]

7.4.3. 1993: Execution of warrants was allowed by the National Crime Authority (NCA) and authorised State agencies: previously all had to be executed by the AFP.

7.5. Since 2003, and subject to fierce debate as evidenced by the number of bills not making it to acts, there have been other changes – notable is the amending legislation of 2006, which introduced 'B-Party' or 'Third Party' Interception Warrants.

7.6. While the TIA sets out the process of approval, reporting requirements and conditions and circumstances for secondary use of any product, the focus of this paper is upon the types of warrant which may be granted and whether these are sufficient for the technology both past, present and future.[59]

7.7. Under the current TIA, the primarily relevant provisions are sections 46 and 46A which deal with telecommunications service warrants and named person warrants respectively.

[58] The section denotes between a number of offence types, under each heading referencing both relevant Commonwealth criminal statutes and those of the States and Territories.
[59] For a process summary, see Sherman, above n 54, 11-13.

7.8. Telecommunications service warrants are granted where other technicalities of the act have been complied with, and notably: (1) that there are reasonable grounds for suspecting that a particular person is using, or is likely to use a particular telecommunications service, (2) that there is information likely to be obtained by intercepting under warrant in communications made to or from the service that would be likely to assist in connection with the investigation of a serious offence or offences in which the person is involved or another person who is likely to be communicated with is involved,[60] having exclusive regard to a number of matters.

7.9. Named person warrants are similar, but instead of telecommunications services, they refer to devices that a person is using or likely to use.

7.10. Named persons warrants were introduced to solve one of the problems of identification: a trend amongst criminals of (knowing the traditional phone service warrant method) carrying a large number of SIM cards and frequently swapping them.[61] Obviously, with technology shifting away from number or service oriented devices and towards hardware with access to many, this is an issue.

7.11. It may be said that given the Pre-Paid Determination, the paper trail of contract phones, and the measures taken to prevent the usefulness of stolen or lost mobile phones, the Act is safe in that respect. However,

[60] Also known as 'B-party' or 'Third Party' Interception. This has the additional requirement under s 46(3) that this kind of interception may only go ahead where all other means of identifying services used have been exhausted, or interception is not otherwise possible.
[61] Up to 80 or more: above n 54, 16.

traded SIM cards or second-hand SIM cards are unlikely to be covered adequately by any of these measures, which was noted by Blunn as being a reason for calling for an indelible and unique device identifier.[62]

7.12. Considering the hypothetical situation posed, things look worse. The lack of indelible and unique device identifiers for PDA's and smartphones [3.10 above], it may be that the legislation is beginning to become outdated not via 'future-proofing' of sections but by sitting atop a philosophical base which is itself becoming outdated.

7.13. In the future, it may make more sense to refer to particular software services such as Skype.[63] Many such services (and likely more as time progresses) however utilise encryption processes, which brings us to the next topic.

8. Data Capture and Understanding

8.1. While Blunn initially identifies these two issues separately, he goes on to discuss them as one.[64] As an issue, this is effectively what they are, and for legislation Parts 14 and 15 of the TA are relevant.

8.2. The TA in sections 331 and 317 provides simplified outlines of the two parts, which relate to the obligations of carriers and carriage service providers and their obligations with respect to national security and law enforcement agency co-operation respectively.

[62] Above n 31, 45.
[63] Above n 4.
[64] Above n 31, 47.

8.3. With respect to National Security, the TA requires that carriers and carriage service providers do their best to prevent the use of their facilities to commit offences, and provide help as reasonably necessary for the purposes of law enforcement, national security and protecting the public revenue.

8.4. With respect to Agency Co-operation, carriers and carriage service providers must comply with obligations concerning interception capability, which involves preparation and submission of annual interception plans and aiding where possible law enforcement agencies.

8.5. While the introduction of B-Party interception has been hotly contested by Electronic Frontiers Australia,[65] on the basis that there is no justification advanced for its introduction, the hypothetical posed illustrates how this kind of interception may be useful. Where a suspect is using a device or account that is completely untraceable or unknown, but for example the wireless hotspot being used is, relevant connection data for the hotspot could be monitored. While there is the issue of privacy and number of users involved – in the situation of the access of specific websites, it may be possible to restrict the data converted into useable product to the offenders type. Proper analysis of data may avoid embarrassing situations such as that encountered in the child pornography

[65] Above n 34, [4.1].

investigation that ultimately resulted in the arrest of the original suspect's neighbour.[66]

8.6. Taking into account the dramatic increase in the up-take of wireless networks of both the 'wireless hotspot' variety, and the home wireless network variety,[67] as well as the demonstrated criminal or probing interest in such networks,[68] even in South Australia,[69] the issue is likely to come to the fore in the near future. Current hotspots (or home networks) do not need to meet any licensing or other legislative arrangements.[70] Possible attempts to control the situation might include banning insecure networks – but this would have to involve governments and law enforcement policy makers being a part of the design process of technology before it is released to the market, and ultimately achieve little. It would seem that given the existing implementation and worldwide standards, it is arguably too late to effect regulation here.

9. Encryption

9.1. Obviously, while data capture may be intercepted, any such data capture will only be useful if it is in an understandable form. The largest likely future obstruction to law enforcement here is encryption. Illustrating the

[66] Below n 69, 5.
[67] Atsushi Umino, *'Development of Wireless Local Area Networks in OECD Countries'* (Paper presented at the Working Party on Telecommunications and Information Services Policy, Directorate for Science, Technology and Industry, 16th April 2003) 11.
[68] Ibid, 8.
[69] Gregor Urbas and Tony Krone, 'Mobile and wireless technologies: security and risk factors' (2006) 329 *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*, 4.
[70] Australian Communications and Media Authority, *Wireless LANs in the 2.4GHz band FAQs* (2007) Australian Communications and Media Authority website <http://www.acma.gov.au/WEB/STANDARD//pc=PC_1794#laws> at May 30th 2007.

way the issues build upon one another – identification and data capture are of little use where the data itself is encrypted such that it cannot be decoded – or at least in a quick amount of time. Arguably, if anything is to be a third issue of concern with respect to law enforcement, it is *timeliness*: encryption is relevant insofar as it affects the real-time interception capabilities. Given that many of the crimes that agencies like the AFP will be interested in will be time sensitive, as in the hypothetical above, this is an issue of extreme relevance.

9.2. While there is perhaps more literature on this single issue than anything else, the Australian response has already extended to what is widely regarded as the realistic limit.[71] The *Cybercrime Act 2001* inserted section 3LA into the *Crimes Act 1914* which allows a magistrate to require a specified person to do, amongst other things, convert the data into documentary form. The effect of this is to remove the right to silence on the topic of encryption keys, and where used compel parties to provide the keys or face the correlating offence's penalty of 6 months.

9.3. This was a possibility suggested in the infamous Walsh report, amongst others.[72] The other solutions commonly suggested – namely Trusted Third Party or Key Escrow or Public Key systems that allow 'backdoors' into the encryption have rightly been widely dismissed on the basis that criminals are unlikely to be swayed by the benefits of such arrangements

[71] See generally above n 31; also above n 16.
[72] See above n 5; Nick Ellsmore, *'Cryptology: Law Enforcement & National Security vs. Privacy, Security & The Future of Commerce'* (1997) 69.

and are likely to actively avoid using them.[73] Additionally, that encryption's effect on the otherwise insecure internet has allowed great advances to be made in areas such as online banking cannot be overlooked: the benefits outweigh the cost.

9.4. Because security packages are increasingly coming preinstalled with software such as Windows, or ancillary on software like Skype, and increasingly easy to implement, law enforcement will have to simply face that encryption is here to stay.

10. Possible Solutions

10.1. Because of the technology-neutral language employed by the various provisions, combined with the increasing tendency to draw up offences in a very broad manner – especially where computers or telecommunications are involved – it has been shown that there is little to no undue limitation upon law enforcement authorities. As can be seen from the issues explored, while there is no definitive direction for future technological advance, technology is on all evidence moving more towards the means of communication utilised in the hypothetical. It may thus be that portions of the legislation become outdated not through a failure to future-proof particular provisions, but a failure to future proof the philosophical conception upon which the legislative schemes are based.

[73] Ellsmore Ibid, 88.

10.2. Conclusions can be drawn. What is illustrated time and again is that the interplay between the legislation, the criminals and law enforcement all takes place *after* the introduction of technology and/or software. It is no surprise then that a theme running throughout much of the literature – especially in the findings or recommendations of what should be done in the future is that the best angle of attack for law enforcement agencies and governments alike is not to wait until the legislative stage at all.

10.3. Especially for the wireless network problem aspect, the problem of easily accessed unsecured networks shows that there are two ways government and law enforcement agencies can get involved and ensure at the least that criminals do not enjoy an undue upper hand.

10.3.1. The first becomes evident from the prevailing tradition where in implementing new technology, security is added on, often as an afterthought – or worse, after a breach – in new technology by both designers (recall the simple analogue problems above) and consumers (using poor security themselves and leaving themselves at risk of identity or machine theft) alike. This is to get involved with standards organisations and ensure that law enforcement and security are adequately represented at the design table from inception.[74]

[74] This is supported by Peter Ford, *'Information Security, Censorship and Privacy'* (Paper presented at the AIC 'IT in Government' Conference, Hyatt Hotel, Canberra, 19th June 1996) 11.

10.3.2. The second becomes evident from the first, and that is that the 'cone of silence' policy adopted after the release of the Walsh report is simply unacceptable. (Hiding the 'unpalatable truths' of issues like encryption on the basis of national security and other reasons.)[75] If criminals are likely to be driven to such means because of the crackdown on traditional mobile phone telephony anyway,[76] public education may go some way to making people realise the dangers involved and take measures to at least curb any possible advantage given to them.

10.4. Given that circumstances like those put forward in the hypothetical are not only a looming future but technology available today, it may be wise to look afresh at Federal policy – particularly in relation to encryption – so that such approaches can be taken and implemented.

[75] The circumstances of this 'coverup' are best summarised by Greg Taylor, 'Burn that book! Canberra spooks lose the plot on 'secret' crypto report' [1999] 5 *Privacy Law and Policy Reporter* 145.
[76] Support for this idea can be found in Russel G. Smith, Nicholas Wolanin and Glenn Worthington 'e-Crime Solutions and Crime Displacement' (2003) 243 *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*, 1.

BIBLIOGRAPHY

Articles/Books/Reports

- Sung-il Ahn, *'Development of Voice over Wifi by integrating Mobile Networks'* (Paper presented at the TISP Working Party, OECD, 29-30th November 2004)
- Australian Federal Police, '*Mobile phone crime brings new challenges in emerging trends for law enforcement*' (1998) Platypus Magazine
- Suzanne Briscoe, 'The Problem of Mobile Phone Theft' (2001) 56 *Crime and Justice Bulletin: Contemporary Issues in Crime and Justice*
- Nick Ellsmore, *'Cryptology: Law Enforcement & National Security vs. Privacy, Security & The Future of Commerce'* (1997)
- Peter Ford, *'Information Security, Censorship and Privacy'* (Paper presented at the AIC 'IT in Government' Conference, Hyatt Hotel, Canberra, 19th June 1996)
- P.N. Grabosky, Russel G. Smith and Paul Wright, 'Crime and Telecommunications' (1996) 59 *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*
- Graham Greenleaf, 'An Endnote on Regulating Cyberspace: Architecture vs Law?' [1998] *University of New South Wales Law Journal* 52
- Graham Greenleaf, 'Privacy and Australia's new Federal Government' [1996] *Privacy Law and Policy Reporter* 14
- Graham Greenleaf and Nigel Waters, 'Scene 5' [1999] 5 *Privacy Law and Policy Reporter* 163
- David Gross, *'Information Security in a Networked World'* (Paper presented at the OECD Workshop, Tokyo 12-13 September 2002)
- Patrick Gunning, 'Distributing encryption software by the Internet: loopholes in Australian export controls' [1998] *Privacy Law and Policy Reporter* 42
- Maria Helena Barrera and Jason Montague Okai, 'Digital Correspondence: Recreating Privacy Paradigms' [1999] 6(2) *Murdoch University Electronic Journal of Law* 14
- Justice Michael Kirby, *'OECD Cryptography Guidelines in context'* (Paper presented at the International Symposium on the Public Voice and the Development of International Cryptography Policy, Carte De Conference International, Paris, France, 25th September 1996)
- Legal Information Access Centre, 'Encryption' [2001] *Hot Topics* 2(10)
- Tony Krone, 'A Typology of the Online Child Pornography Offending' (2005) 279 *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*
- Tony Krone, 'International Police Operations Against Online Child Pornography' (2005) 296 *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*
- Russel G. Smith, 'Preventing Mobile Telephone Crime' (1996) 54 *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*
- Russel G. Smith, Nicholas Wolanin and Glenn Worthington 'e-Crime Solutions and Crime Displacement' (2003) 243 *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*
- *SIFT Notes* 2005-05
- Greg Taylor, 'Burn that book! Canberra spooks lose the plot on 'secret' crypto report' [1999] 5 *Privacy Law and Policy Reporter* 145
- Kim Wheatley, 'Nitschke admits to secret death code', *The Advertiser* (South Australia), May 2 2007

- Gregor Urbas and Tony Krone, 'Mobile and wireless technologies: security and risk factors' (2006) 329 *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*
- Atsushi Umino, *'Development of Wireless Local Area Networks in OECD Countries'* (Paper presented at the Working Party on Telecommunications and Information Services Policy, Directorate for Science, Technology and Industry, 16th April 2003)

Legislation

- *Criminal Code Act 1995* (Cth)
- *Crimes Act 1914* (Cth)
- *Cybercrime Act 2001* (Cth)
- *Telecommunications Act 1997* (Cth)
- *Telecommunications (Interception) Act 1979* (Cth)
- *Telecommunications (Interception and Access) Act 1979* (Cth)
- *Telecommunications (Service Provider - Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000* (Cth)

Other Sources

- ACMA Fact Sheet [FS 21] 'Compliance with identity check process for pre-paid mobile phone services'
- ACMA Fact Sheet [FS 100] 'Voice over internet protocol equipment regulation'
- ACMA Fact Sheet [FS 104] 'Wireless local area and metropolitan networks, and the Deployment of Mobile Phone Network Infrastructure Code'
- Anthony S. Blunn: Commonwealth, Attorney General's Department: Public Affairs Unit, *'Report of the review of the regulation of access to Communications*' (2005)
- Bills Digest no 133 2004-5 Criminal Code Amendment (Suicide Related Material Offences) Bill 2005
- Commonwealth, Information and Security Law Division Attorney General's Department per Peter Ford, *Telecommunications Interception Policy Review* (1999)
- Commonwealth, Tom Sherman, *Report of review of named person warrants and other matters* (2003)
- Commonwealth, Gerard Walsh, *Review of Policy relating to Encryption Technologies* (1997).
- Commonwealth, Department of Communications, Information Technology and the Arts, *Review of the Regulation of Content Delivered over Convergent Devices* (2006)
- Explanatory Memorandum, Crimes Legislation Amendments (Telecommunications Offences and Other Measures) Bill 2004 (Cth)
- Explanatory Memorandum, Criminal Code Amendment (Suicide Related Material Offences) Bill 2005 (Cth)
- Telecommunications Legislation Amendment Bill 1997, Second Reading 19th November 1997
- Interview with Anonymous Technical Support Officer, - personal details withheld for anonymity reasons, Optus (Telephone interview, 18th May 2007)
- Interview with Police Constable – identity and date withheld for privacy reasons.

Web Resources

- Australian Communications and Media Authority, *Wireless LANs in the 2.4GHz band FAQs* (2007) Australian Communications and Media Authority website <http://www.acma.gov.au/WEB/STANDARD//pc=PC_1794#laws> at May 30th 2007
- AMTA, *'Check the Status of Your Handset'* <http://www.amta.org.au/default.asp?Page=405> at May 22 2007
- AMTA, *'Mind Your Mobile'* <http://www.amta.org.au/default.asp?Page=132> at May 22 2007
- Bruce Schneier, *'The Architecture of Security'* <http://www.schneier.com/essay-131.html> at 19 May 2007
- Bruce Schneier, *'A Sci-Fi Future Awaits the Court'* <http://www.schneier.com/essay-089.html> at 19 May 2007
- Bruce Schneier, *'Your Vanishing Privacy'* <http://www.schneier.com/essay-109.html> at 19 May 2007
- EFA, *'Submission to the Parliamentary Joint Committee on the National Crime Authority: Inquiry into the Law Enforcement Implications of New Technology'* <http://www.efa.org.au/Publish/ncasub.html> at 10 May 2007
- EFA, *'Submission to the Senate Legal and Constitutional Legislation Committee "Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006'* (2006) <http://www.efa.org.au/Publish/efasubm-slclc-tiabill-2006.html> at May 23 2007
- EFA, *'The Australian Crypto FAQ'* <http://www.efa.org.au/Issues/Crypto/cryptfaq.html> Accessed 10 May 2007
- GSM Favourites, *Introduction to SMS* <http://www.gsmfavorites.com/documents/sms/introduction/> at 22 May 2007
- HPC Factor: *CESDC0033 – Windows CE 2.0 and Ethernet / Wireless Network Connectivity* <http://www.hpcfactor.com/support/cesd/c/0033.asp> at 22 May 2007
- HPC Factor: *The History of Microsoft Windows CE* <http://www.hpcfactor.com/support/windowsce/> at 22 May 2007
- Internode, *News and Media: Adelaide to Boost Free Wireless Web Reach by 250%* (2007) <http://www.internode.on.net/about/news/20060808-citylan.htm> at 1 June 2007
- Internode Wireless Hotspot information site: <https://hotspot.internode.on.net/>
- Microsoft Windows Mobile website: <http://www.microsoft.com/windowsmobile/default.mspx>
- Skype for Pocket PCs: <http://www.skype.com/download/skype/mobile/> at 14 May 2001