To what extent is the right of privacy protected under the Telecommunications (Interception and Access) Act 1979 (Cth)?

น.ส.สาวเสียรพร วงศ์ก้านหนองหว้า[1]

Introduction

It is generally accepted that the electronic surveillance is very helpful device in a criminal investigation. It can provide a highly reliable means, cost-effective result of identifying suspects and corroboration of evidence collected by less reliable resource.[2] However, the unrestrained use of electronic surveillance may infringe the right of privacy. It could be seen that there are legislations to control the use of electronic surveillance in order to protect the right of privacy; however, in recent years, trend has been shifting away from protection of privacy right to authorizing government agencies greater access and surveillance. Accordingly, the right of privacy in communications may not be well protected under the Telecommunications (Interception and Access) Act 1979 (Cth) ("TIA Act"). This essay attempts to study whether the TIA Act, in particular the Telecommunications (Interception) Amendment Act 2006 ("the 2006 Act") undermines the protection of privacy which is one of its original policy objectives. Moreover, the paper will examine some loopholes in the law.

---

[1] นิติศาสตรบัณฑิต สำนักวิชานิติศาสตร์ มหาวิทยาลัยวลัยลักษณ์
นิติศาสตรมหาบัณฑิต (นิติศาสตร์มหาบัณฑิต) คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
นิติศาสตรมหาบัณฑิต (นิติศาสตร์มหาบัณฑิต) มหาวิทยาลัยเกษตรศาสตร์
ผู้พิพากษาสมทบ รุ่นที่ 51
LL.M. Cambridge University, England (2001-2002)
LL.M. King' College, University of London, England (2002-2003)

[2] Simon Bronitt, 'Contemporary Comment- Electronic Surveillance and Informers: Infringing the Right to Silence and Privacy (1995) 20 Criminal Law Journal 166 at 166.

Privacy in Communications

Warren and Brandeis noted privacy as the 'right to be let alone'.[3] In similarity, there is a view that 'man's home is his castle' and 'the poorest man may in his cottage bid defiance to all the forces of the Crown'.[4] Moreover, the United Nations Declaration of Human Rights at Article 12 provides that every individual has a right to privacy. Nonetheless, it does not define the meaning of 'privacy'. The Australian Law Reform Commission accepted that the concept is elusive and despite numerous attempts a satisfactory definition of privacy has never been achieved.[5] Without the general standard meaning of the word 'privacy', it could therefore be said that the extent to which the meaning of 'privacy' relies on nation's culture. However, it could be seen that privacy rights are principally and undeniably individualistic. It forms an essential part of a functioning community. Without privacy, people may feel inhibited from forming close relationships within the family or outside in social groups. Therefore, it is privacy that facilitates the social spheres to function. Privacy invasion can be classified into four main types:

(a) intruding upon a subject's solitude and personal operations;

(b) information gathering in an individually identifiable manner against the wishes or without the knowledge of the subjects;

(c) interfering through use of information gathered without consent to create a situation hostile to the attainment of that individual's desired goals;

(d) violating accepted standards by impinging on the sanctity of important private relationships that are endorsed by the ambient culture.[6]

Legal Protection of Privacy Right in Communications in Australia

In general, there are two main kinds of electronic surveillance: listening devices ('bugging') and telecommunications ('tapping'). The law governing electronic surveillance is split between Commonwealth law, which exclusively governs the interception of telecommunications, and State and Territory law, which governs the interception of private communications by any other means.[7] The boundary between two Acts is that once it is out of circumstances that the TIA Act applies the State and Territory law

---

3 Simon D. Warren & Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.
4 Warwick Smith, 'Telecommunications and Privacy' (1994) Telecommunications Law & Policy Review 36.
5 Australian Law Reform Commission, Privacy (Report No. 22) (1983) at 19-20.
6 JK Katz, 'Social-Political Response to Technological Advances' (1980) 12 (4) Telecommunications Policy 353.
7 Bronitt, above nt at 146.

such as the Listening Devices Act 1984 (NSW) will apply. The basic rule of legislative interpretation is that a valid law of the Commonwealth will prevail over an inconsistent State and Territory law to the extent of the inconsistency.[8] This rule is well supported by the authority in *Miller*.[9]

Protection of Privacy under the Telecommunications (Interception and Access) Act 1979 (Cth)

The primary objective of the TIA Act is to protect the privacy of individuals who use the Australian telecommunications system. TIA Act is to specify the circumstances in which it is lawful for interception of, or access to, communications that take place.[10] In brief, the TIA Act prohibits the interception of communications passing over a telecommunications system and prohibits access to stored communications (i.e. email, SMS and voice mail messages stored on a carrier's equipment) except where authorized in specified circumstances. The primary exception is to enable law enforcement agencies to lawfully intercept or access telecommunications in specified circumstances pursuant to an interception warrant or a stored communications warrant issued under the TIA Act.[11]

Section 7(1) of the TIA Act sets out the prohibition:

A person shall not:

(a) intercept;

(b) authorise, suffer or permit another person to intercept; or

(c) do any act or thing that will enable him or another person to intercept; a communication passing over a telecommunications system.

It is an offence if violating this section and punishable by a fine or imprisonment under section 105. Moreover, under section 107 A, a person can recover civil damages caused by an unlawful interception.

It is worthy noting that before 13th June, 2006, it was the Telecommunications (Interception) Act 1979 and this name was changed to the TIA Act by the 2006 Act. Due to the technology advance, one would expect the law enforcement agencies to have sufficient authority to deal with it. Even though between 15th December, 2004 and 12th June 2006, the Telecommunications (Interception) Act 1979 did not apply to 'stored communications' such as email, voice mail messages, and SMS that are stored on the equipment of carrier, the 2006 Act later broadened the scope of the Act to cover the 'stored communications' held by a telecommunications carrier Also, the 2006 Act established the provisions of

---

[8] Alan J. Collier, 'When Does Unauthorised Listening Become Interception?' (1994) 68(1) Law Institute Journal 59 at 59.

[9] Miller v Miller (1979) 141 CLR 269.

[10] Telecommunications Interception & Access Laws (2006) Electronic Frontiers Australia < http://www.efa.org. au/Issues/Privacy/tia.html> accessed 18 April 2008.

[11] Ibid.

a new stored communications warrant. Arguably, the 2006 Act brought 'a sea-change in regulatory design'.[12] From section 7(1), the question may arise as to what conduct constitutes the 'interception'. Subject to section 6(1), interception of a communication takes place when there are: (a) listening to or recording, by any means; (b) a communication; (c) in its passage over a telecommunication system; and (d) without the knowledge of the person making the communication.[13] While the definition of 'record' is defined as a record or copy, whether in writing or otherwise, of the whole or a part of the communication, the word 'listen' is not defined. Under section 5, 'communication' covers conversations and messages and any part of a conversation or message in whatever forms they are realized such as speech data, text, visual images and so on. Therefore, the TIA Act applies to communications that are passing over a telecommunication system. In order to clarify the debate on the issue of passing over a telecommunications system, the meaning of the term 'passing over a telecommunications system' was amended by the 2006 Act. The live or real-time communications over a telecommunication system such as conversations over telephone calls and communications in transit over the Internet are subject to the TIA Act.

With regard to the protection of privacy right, firstly, the TIA Act does not only protect the actual act of interception but it also protects all information obtained from the illegal interception. Section 63 of the Act prohibits communication to another, the making use of, making a recording of, or giving in evidence in proceeding information even if it is obtained lawfully, but in contravention of section 7(1). It could be seen that section 63 reveals the guarantee of the privacy right. It is reasonable that if the method to obtain such information is illegal, taking any advantage from such information should be prohibited. Similarly, under section 77, its main purpose is to curtail the proceedings in which intercepted information may be used, whether or not it is obtained in contravention of section 7(1).

Secondly, the warrant system is very important to guarantee against state abuse of electronic surveillance, and provides safeguards which must be complied with before the warrant is issued.[14] Under the TIA Act, there are two main purposes for the interception warrants to be made: (a) national security and (b) law enforcement. For the former purpose, the Australian Security Intelligence Organization ('ASIO') can intercept communications under the Chapter 2 Part 2-2 of the TIA Act which provides that the

---

[12] *Simon Bronitt & James Stellios, 'Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?'(2006) 24 (4) Prometheus 413 at 414.*

[13] *Telecommunications (Interception and Access) Act 1979 (Cth) ('TIA Act'), section 5.*

[14] *Simon Bronitt, "Electronic Surveillance, Human Rights and Criminal Justice" (1997) 3 Australian Journal of Human Right 183.*

Attorney-General may issue warrants to ASIO where the communications are being used by a person who is reasonably suspected of engaging in activities prejudicial to security, and the interception will, or is likely to, assist the ASIO in its function of obtaining intelligence relevant to security. Moreover, due to the warrants, ASIO can gain access to stored communications.[15] However, it could be argued that the Attorney-General as a gatekeeper is not an independent judicial; therefore, his conduct may be affected by political imperative. For the latter purpose, the interception warrants may be issued in accordance with Chapter 2 Part 2-5 of TIA Act to specified criminal law enforcement agencies in order to investigate serious crime only. The 'serious offences' is defined in section 5D.

Thirdly, there are two types of interception warrants under the TIA Act: (a) a telecommunications service warrant and (b) a name person warrant. While the former authorizes the interception of only one service at a time[17], the latter authorizes the interception of more than one telecommunications services used or likely to be used by the person the subject of the warrant.[18] However, for both warrants, the 2006 Act introduced 'B-party interception' which is interception of a service that is likely to be used by another person (a non-suspect) to communicate with the suspect. The argument is whether this legislation goes further than its justification. Is this provision proportionate to its objective of the TIA Act? One takes a view that after considering a connection between the use of the non-suspect or innocent third party's telecommunications service and the security or law enforcement objective, the 'B-Party' thresholds are low.[19] Under sections 9 (1) (a) (ia) and (b) and 46 (1) (d) (ii), warrants may be issued where it is 'likely' that monitoring the communication of a B-Party or services used by third parties will intercept communication by a person of interest. It could be understood in case of interception of a person who is already a suspect in investigation. However, in case of B-party interception, there are highly possible to intrude into one's privacy right since the provisions allow the government agencies to collect and pore over all the communications between non-suspect and anyone with whom the non-suspects communicate such as family, closed friends, doctors.[20] It would seem to me that the legislation goes too far and there is less justification to do so because individual expects the conversations over telecommunications to be private and confidential to the participants without intrusion by state and

[15] *TIA Act, section 109.*
[16] *David Hume & George Williams, 'Who's Listening? : Intercepting the Telephone Calls, Emails and SMS's of Innocent People'(2006) 31(4) Alternative Law Journal 211 at 212.*
[17] *TIA Act, section 46.*
[18] *TIA Act, section 46A.*
[19] *Bronitt & Stellios, above n11 at 417.*
[20] *Hume & Williams, above n16 at 212.*

commercial interests. Nonetheless, the limitations of this expectation could be accepted where there are prevailing interests like a national security and law enforcement. Arguably, interception is not based on reasonable suspicion but the statutory threshold would be satisfied by mere involvement in broad category offences where the subject is typically called as a 'person of interest'.[21] In Blunn Report, it accepted the privacy protection issue in using B-Party interception and viewed that B-Party interception must not be used for fishing expeditions.[22]

Fourthly, the 2006 Act inserted amendment to enable 'Equipment-based interception', which is interception of communications made by way of a particular telecommunications device that a person is using or is likely to use. However, the argument is that allowing to do so is an inappropriately and unjustifiably high potential to cause interception of communications of non-suspect (such as the person whose name is not in the warrant) since the types of device numbers to be used do not necessarily uniquely identify a particular device.[23]

Fifthly, it could be argued that sections 9 and 46 of the TIA Act do not limit the aims to which the information collected under warrant can be put.[24] Thus, it is likely that a person entirely unrelated to the original suspect (non-suspect person) may be investigated or prosecuted merely because he or she talks to a suspect or someone who talked to a suspect.[25] Of course, the privacy right of individual is destroyed due to the accidental relationship. It could be further argued that there are no limitations as to the identity of the innocent party, the intercepted communication content or the identity of other parties to the intercepted communication.[26] As a result, it is questionable whether such the expanded power is justified when weighed against a legitimate problem of public policy, in particular war on terror. Sixthly, an eligible judge[27] or nominated Administrative Appeals Tribunal members[28] have authority to issue interception warrants. It could be noticed that the proceedings to issue the warrant are conducted ex parte. Judges hear the evidence only from

---

[21] Bronitt & Stellios, above n11 at 416.
[22] Anthony Blunn, Report of the Review of the Regulations of Access to Telecommunications (2005) at 76 ('Blunn Report').
[23] Inquiry into the Provisions of the Telecommunications Amendment Act (2006) Electronic Frontiers Australia < http://www.efa.org.au/Publish/efasubm-sicic-tiabill-2006.html#47_32> accessed 18 April 2008.
[24] Hume & Williams, above n15 at 212.
[25] Id at 213.
[26] Bronitt & Stellios, above n11 at 417.
[27] TIA Act, section 6D.
[28] TIA Act, section 6DA.

the officials. It is questionable how the privacy of the suspects will be protected if they do not even have a chance to speak. Moreover, in *Grollo v Palmer*[29] the High Court held that 'eligible judges' as defined by the Telecommunication (Interception) Act 1979 to issue warrants are acting in a non-judicial capacity. Consequently, the warrants issued could not be reviewed. Although there are some judgments showing that the issue of warrants is not in the scope of the review, a different view is that these decisions should be subject to judicial review.[30]

Seventhly, Australia became a signatory to the International Covenant on Civil and Political Rights on 18th December 1972 and ratified it on 13th August 1980. This means that Australian government acknowledges the standard therein. With regard to electronic surveillance, Article 17 provides:

(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

(2) Everyone has the right to the protection of the law against such interference or attacks.

It could be argued that the issues concerning surveillance are relevant to issues of privacy. Should the Australian government therefore keep in mind when making any changes to laws concerning surveillance?

Eighthly, with regard to interception of 'stored communications' held by a telecommunications carrier including Internet Service Providers, the stored communications warrants may be issued by a much broader number of authorities, including agencies that enforce pecuniary penalties or administer revenue laws. The argument is why a different standard of issue of interception warrants and stored communications warrants. The Victorian Privacy Commissioner views that 'emails are....in need of a high level of protection. Communication by email is fast becoming the norm... An essential requirement for the development of a trustworthy and effective communications network is an assurance'.[31] The argument is that individuals especially the young much rely on stored communications for private and intimate conversation in the same way they would make on a telephone conversation and communication by email over the Internet is intended to be private

---

[29] *Grollo v Palmer (1995) 184 CLR 348.*

[30] *Bronitt, above nt3 at 195.*

[31] *Parliament of Australia, Submission to Senate Legal and Constitutional Legislation Committee (2004).*

because the sender intends to email to be read by only the recipients. It is likely to see that reading email of someone is as intrusive as intercepting a voice telecommunication. Hence, should stored communication be subject to an equivalent level of privacy protection to a real-time communication? Doubtfully, why would the government seek to protect interception of live communications more than 'stored communications'?

Ninthly, there is also a difference between stored communications and interception warrants concerning the offences that each covers. The question put forward is why stored communications warrants may be issued for a lesser range of offences and civil penalties. Moreover, the reporting requirements for stored communications warrant are less strict. Is it possible to justify whether the interception warrant is mindful of access to private communications than the other?

Finally, in respect of 'overt access to stored communication', under section 108 of the TIA Act, the access to the stored communications with the knowledge of neither the intended recipient nor the sender of the communication is prohibited. For the purposes of having knowledge of the act, a written notice of an intention to do must be given to the person.[32] It is arguable that allowing access to stored communication where one party is informed may be considered as a regulatory loophole.[33] This is because notification to one party could not change the privacy expectation of the other in the communications.

Conclusion

The concept of privacy is an imprecise one and the multiplicity of meanings may make it difficult to deal with. However, if the privacy right is engaged in a particular case, any interference with that right should be directed towards a legitimate aim. On one hand, the TIA Act is originally designed with the public policy to protect the privacy of communications passing over the telecommunications system and to make the community trust the system integrity. On the other hand, the TIA Act as it currently stands is not in itself an adequate privacy protection. One amongst other issues, the policy justification of accessing stored communications regime under the TIA Act seems to be unclear. If it could be accepted that the TIA Act is to protect the privacy right of individual, the state should be able to justify their reasons for breaching such a right and power to do so should be explicitly detailed. Also, the balance between individual

[32] *TIA Act, section 108 (1A).*
[33] *Bronitt & Stellios, above nn.*

rights of privacy and freedom from intrusion and the legitimate needs of law enforcement agencies must be appropriate. Consequently, if telecommunication privacy rights are to be protected at an acceptable level, amendment to the Act is required to be introduced.

Bibliography

1. Alan J. Collier, 'When Does Unauthorised Listening Become Interception?' (1994) 68(1) Law Institute Journal 59.

2. Angus Henderson & Annemaree McDonough, 'Call Monitoring-Legalities and Regulation' (1999) 2 (8) Telemedia 97.

3. Anthony Blunn, Report of the Review of the Regulation of Access to Communications (2005).

4. Australian Law Reform Commission, Privacy (Report No. 22) (1983).

5. Beverley Schurr, Criminal Procedure NSW (1996).

6. David Hume & George Williams, 'Who's Listening? : Intercepting the Telephone Calls, Emails and SMS's of Innocent People' (2006) 31(4) Alternative Law Journal 211.

7. Ian D. Elliott, 'Listening Devices and the Participant Monitor: Controlling the Use of Electronic Surveillance in Law Enforcement' (1982) 6 Criminal Law Journal 327.

8. Inquiry into the Provisions of the Telecommunications Amendment Act (2006) Electronic Frontiers Australia < http://www.efa.org.au/Publish/efasubm-slclc-tiabill-2006.html#47_32> accessed 18 April 2008.

9. Jame Rachels, 'Why Privacy is Important' (1975) 4 Philosophy and Public Affairs 323.

10. JK Katz, 'Social-Political Response to Technological Advances' (1980) 12(4) Telecommunications Policy 353.

11. Julie De Rooy, 'What's Bugging You?': Increased Interception and Surveillance Powers and The Impact on Privacy' (2005) 79(6) Law Institute Journal 50.

12. Michael Hudson, 'Virtual Privacy-The Impact of Electronic Technology on Communications' (1998) 3 Media & Art Law Review 18.

13. Penelope J. Ward, 'Privacy and Telecommunications – the Impact of Technological Developments' (1995) 3 Telecommunications Law & Policy Review 99.

14. Priscilla M. Regan, Legislating Privacy (1995).

15. Peter Ford, 'Who's Listening? – Recording and Monitoring of Personal and Business Communications' (1998) 48 (2) Telecommunication Journal of Australia 75.

16. Richard A. Posner, 'The Right to Privacy' (1978) 12 Georgia Law Review 393.

17. Robert Chalmers, 'Orwell or All Well? : The Rise of Surveillance Culture' (2005) 30 (6) Alternative Law Journal 258.

18. Roger Magnusson, 'Privacy, Surveillance and Interception in Australia's Changing Telecommunications Environment' (1999) 27 Federal Law Review 33.

19. Simon Bronitt, 'Contemporary Comment-Electronic Surveillance and Informers: Infringing the Rights to Silence and Privacy' (1996) 20 Criminal Law Journal 144.

20. Simon Bronitt, 'Electronic Surveillance, Human Rights and Criminal Justice' (1997) 3 Australian Journal of Human Right 183.

21. Simon Bronitt & James Stellios, 'Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?'(2006) 24 (4) Prometheus 413.

22. Simon Bronitt & James Stellios, 'Telecommunications Interception in Australia: Recent Trends and Regulatory Prospects' (2005) 29 Telecommunications Policy 875.

23. Simon D. Warren & Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

24. Parliament of Australia, Submission to Senate Legal and Constitutional Legislation Committee (2004).

25. Tim Dixon, 'Changing Landscape of Telecommunications Privacy' (2000) 4 Telemedia 13.

26. Telecommunications Interception & Access Laws (2006) Electronic Frontiers Australia < http://www.efa.org.au/Issues/Privacy/tia.html> accessed 18 April 2008.

27. Warwick Smith, 'Telecommunications and Privacy' (1994) Telecommunications Law & Policy Review 36.

28. William Prosser, 'Privacy' (1960) 48 California Law Review 383.