ACCESSING TELECOMMUNICATIONS DATA FOR NATIONAL SECURITY AND LAW ENFORCEMENT PURPOSES

*Sharon Rodrick**

INTRODUCTION

Technological developments, particularly the advent of the Internet and the mobile phone, have spawned a vast increase in the volume, type and availability of telecommunications information.[1] Mobile phones are now capable of sending and receiving SMS text messages and emails, accessing and downloading material from the Internet, taking photographs, streaming video and audio content and providing GPS navigation. National security and law enforcement agencies frequently wish to access telecommunications information for national security and law enforcement purposes. The desired information may be 'telecommunications content' — that is, the actual substance of a communication — or 'telecommunications data' — meaning information about a communication but not the substance of it.

Access to telecommunications information by national security and law enforcement agencies is part of a wider debate about what constitutes an appropriate response to the threat of terrorism and to the use by criminals of increasingly sophisticated methods. Governments in Western democracies have tended to react by conferring on their national security and law enforcement agencies significantly increased powers to obtain information about individuals, including increased access to telecommunications information. Such governments have acted on the premise that citizens expect their government to keep them safe, and to equip itself with the power to do so.[2] However, increased state power is often arrogated at the expense of human rights and freedoms, particularly in Australia, which lacks a Bill of Rights to 'balance

---

* BA, LLB(Hons)(Melb), LLM (Melb), Senior Lecturer in Law, Faculty of Law, Monash University. My sincere thanks go to Dr David Lindsay for his critical comments on an earlier draft of this article, and also to the anonymous referee.

1 New South Wales Council for Civil Liberties, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007*, 11 July 2007.

2 Niloufer Selvadurai, Peter Gillies and Md Rizwanul Islam, 'Maintaining an Effective Legislative Framework for Telecommunication Interception in Australia' (2009) 33 *Criminal Law Journal* 34, 44.

the ledger' between the two.[3] In the context of telecommunications, the freedom most likely to be compromised by increased powers of access is individual privacy.

It is not surprising, therefore, that the debate regarding the extent to which national security and law enforcement agencies should be able to access telecommunications information invariably focuses on the tension between the need to protect the privacy of individuals who use the telecommunications system — particularly those who are suspected of planning or committing crimes or acts of terrorism — and the need to protect national security and facilitate law enforcement. As a matter of principle, it is fairly uncontentious that privacy and national security/law enforcement each have legitimate claims to recognition and protection, and that there are circumstances in which it is justifiable to encroach on the former to protect and promote the latter. The discussion inevitably centres on how the law can best protect society from crime and terrorism while continuing to preserve the rights and freedoms of individuals, or, if both cannot be achieved in adequate measure, which should be given primacy.

Access to telecommunications content and data is primarily governed by the *Telecommunications (Interception and Access) Act 1979* (Cth) (the '*Interception Act*') and, to a lesser extent, by the *Telecommunications Act 1997* (Cth) (the '*Telecommunications Act*'). In deference to the fact that technological advances have made it possible to use the telecommunications system to communicate in a multiplicity of ways, the *Interception Act* creates three broad access regimes. The first pertains to interception of real time communications, primarily voice communications.[4] There is a general prohibition on intercepting live communications — that is, communications as they are passing over a telecommunications system[5] — in the interests of protecting the privacy of the persons who make and receive such communications.[6] However, the prohibition is qualified by a number of exceptions. The primary exceptions allow for warrants to be issued to the Australian Security Intelligence Organisation ('ASIO' or the 'Organisation') and to certain State and federal law enforcement agencies which permit them to intercept telecommunications for national security and law enforcement purposes.[7] Warrants are issued to ASIO by the Federal Attorney-General,[8] and to law enforcement agencies by an 'eligible judge' – namely, a judge of a court created by the Commonwealth Parliament who has consented to being nominated and who has been declared by the

3 Simon Bronitt and James Stellios, 'Telecommunications Interception in Australia: Recent Trends and Regulatory Prospects' (2005) 29 *Telecommunications Policy* 875, 887.

4 *Telecommunications (Interception and Access) Act 1979* (Cth) ch 2.

5 This phrase has been judicially considered in the context of telephone tapping in a number of cases. See, eg, *Miller v Miller* (1978) 141 CLR 269; *R v Curran and Torney* [1983] 2 VR 133; *R v Oliver* (1984) 57 ALR 543; *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222.

6 *Telecommunications (Interception and Access) Act 1979* (Cth) s 7.

7 *Telecommunications (Interception and Access) Act 1979* (Cth) pts 2–2, 2–5.

8 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 9, 9A. Provision is made for warrants to be issued by the Director-General of Security in emergencies: s 10.

Minister to be an eligible judge[9] — or by nominated members of the Administrative Appeals Tribunal ('AAT').[10]

The second regime regulates access to stored communications.[11] These are communications that have completed their passage over the telecommunications system, that are held on equipment that is operated and possessed by a carrier, and that 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.[12] In short, the regime applies to communications that are temporarily stored by the carrier or carriage service provider ('CSP') at some point during the course of their transmission over the telecommunications system before being received by the intended recipient. They include emails, SMS and voice mail messages.[13] The stored communications regime only applies where communications are accessed from the telecommunications service provider; it does not govern access to communications that are stored on equipment in the possession of the intended recipient.[14] Again, in the interests of privacy, there is a general prohibition on accessing stored communications,[15] qualified by another set of exceptions, the most significant ones being the provision for warrants to be issued to ASIO and specified enforcement agencies allowing them to access stored communications for national security and law enforcement purposes.[16] ASIO can access stored communications using its existing interception warrants.[17] Enforcement agencies, however, must obtain a stored communications warrant. These can be issued by an 'issuing authority', being a consenting judge of a court created by the

---

9 *Telecommunications (Interception and Access) Act 1979* (Cth) s 6D. Eligible judges can be drawn from the Federal Court of Australia, the Family Court of Australia or the Federal Magistrates Court.

10 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 46, 46A. The Deputy President, full time and certain part time senior members, and members of the AAT can be nominated by the Minister to issue warrants: *Telecommunications (Interception and Access) Act 1979* (Cth) s 6DA. To be eligible for nomination, part-time senior members and members of the AAT must have been enrolled as a legal practitioner of the High Court, the Federal Court or a State or Territory Supreme Court for no less than five years.

11 *Telecommunications (Interception and Access) Act 1979* (Cth) ch 3.

12 *Telecommunications (Interception and Access) Act 1979* (Cth) s 5.

13 See Tonia Starey, 'Getting the Message: A Comparative Analysis of Laws Regulating Law Enforcement Agencies' Access to Stored Communications in Australia and the United States' (2005) 10 *Media and Arts Law Review* 23, 24–26. It appears that Instant Messaging systems fall outside the stored communications regime: Selvadurai, Gillies and Islam, above n 2, 42. See also fn 90.

14 Explanatory Memorandum, Telecommunications (Interception) Amendment Bill 2006 (Cth) 4. Access to communications that are stored on a person's mobile phone or computer can be procured pursuant to other lawful access arrangements, such as a general search warrant.

15 *Telecommunications (Interception and Access) Act 1979* (Cth) s 108.

16 *Telecommunications (Interception and Access) Act 1979* (Cth) pts 3–2 , 3–3.

17 *Telecommunications (Interception and Access) Act 1979* (Cth) s 109. Section 109 expands the authority of an interception warrant to cover stored communications provided the warrant would have authorised interception of the communication if it were still passing over a telecommunications system.

Commonwealth Parliament, a Federal Magistrate, a magistrate, and by nominated members of the AAT.[18]

When deciding whether to issue an interception or stored communications warrant to a law enforcement agency, the relevant issuing authority must have regard to the extent to which methods of investigation that do not involve interception or access are available or have been used by the applicant, and how much the interception or access of a target person's communications would interfere with their privacy.[19]

The third regime regulates access to telecommunications data, which loosely refers to 'traffic' or 'transactional' data, that is, information *about* a communication rather than its content.[20] It is with this regime that this paper is primarily concerned. While perhaps not as useful to national security and law enforcement agencies as the actual substance of a communication, telecommunications data can provide these agencies with valuable information about a person's pattern of communications and location. The access scheme for telecommunications data requires an understanding of Part 13 of the *Telecommunications Act,* and Chapter 4 of the *Interception Act*. The former is concerned with protecting the confidentiality of communications. It does so by imposing a general prohibition on the disclosure and use of information by providers of telecommunications services. However, the disclosure and use of this information is authorised in certain enumerated circumstances. Until recently, both the general prohibition and all of the exceptions were contained in the *Telecommunications Act*, including exceptions permitting the disclosure and use of telecommunications data for national security and law enforcement purposes.[21] However, in 2005, the *Report of the Review of the Regulation of Access to Communications* (the 'Blunn Review') concluded that the distribution of provisions between the *Telecommunications Act* and the *Interception Act* dealing with access to telecommunications data for security and law enforcement purposes was 'complicated, confusing and dysfunctional'.[22] It recommended that the law enforcement and national security provisions be shifted to the *Interception Act*, thereby making that Act a single, comprehensive Act containing the framework for national security and law enforcement agencies to access all forms of telecommunications information.[23] This recommendation was implemented in 2007 when the exceptions permitting disclosure and use of telecommunications data for national security and law enforcement purposes were removed from the *Telecommunications Act* and transferred to Chapter 4 of the *Interception Act* by the

---

18 *Telecommunications (Interception and Access) Act 1979* (Cth) s 5 (definition of 'issuing authority'). The Minister can nominate the Deputy President and certain full or part time senior members, and members of the AAT to issue warrants: *Telecommunications (Interception and Access) Act 1979* (Cth) s 6DB.

19 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 46(2)(a),(d), 46A(2)(a),(d), 116(2)(a),(d).

20 *Telecommunications (Interception and Access) Act 1979* (Cth) ch 4. The boundary between the substance of a communication and information about a communication is not easily defined. This issue is addressed at length below.

21 The national security and law enforcement exceptions were contained in ss 282 and 283 of the *Telecommunications Act 1997* (Cth).

22 Anthony Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) 6.

23 Ibid 10 (Recommendation (i)). See also, Senate Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, *Telecommunications (Interception and Access) Amendment Bill 2007 [Provisions]* (2007) [1.3].

Telecommunications (Interception and Access) Amendment Act 2007 (Cth). The other exceptions remain in the *Telecommunications Act* and are expressly preserved by s 173 of the *Interception Act*.[24] It should be noted that the *Telecommunications (Interception and Access) Amendment Act 2007* (Cth) did not effect a mere transfer of provisions from the *Telecommunications Act* to the *Interception Act*. There are some significant modifications and additions to the exceptions, many of which are controversial. Moreover, the transfer of provisions has reignited some of the contentious issues that were in existence even when the provisions were located in the *Telecommunications Act*.

The purpose of this paper is to outline the circumstances in which telecommunications data can be lawfully accessed for national security and law enforcement purposes, and to consider whether this access regime sacrifices individual privacy to an unacceptable extent. Since privacy is the primary public interest against which the telecommunications data regime must be evaluated, this paper will begin with a brief exploration of the importance of privacy in the telecommunications context. The paper will then outline the provisions of Part 13 of the *Telecommunications Act* before proceeding to describe and critique both structural and operational aspects of the telecommunications data regime, primarily from a privacy perspective. Many of the deficiencies of the regime were identified in submissions made to the Senate Standing Committee on Legal and Constitutional Affairs (the 'Senate Committee' or 'Committee') which conducted an inquiry into the provisions of the Telecommunications (Interception and Access) Amendment Bill 2007 (Cth). This paper will draw on those submissions and make suggestions for reform across a number of areas. While not directly concerned with the interception and stored communications regimes, some tentative comments as to whether the divergence in protections between these regimes and the telecommunications data regime is justified will be interspersed throughout the paper.[25]

THE LINK BETWEEN PRIVACY, TELECOMMUNICATIONS INFORMATION AND THE STATE

The balancing approach

Many governments, policy makers and academic scholars evaluate legislative regimes that seek to protect national security and enhance law enforcement at the expense of human rights on the assumption that it is both possible and appropriate to resolve the tension between public safety and individual liberty by striving to achieve a balance between the two.[26] Others maintain that a balancing approach is inherently flawed.

---

24 In a similar vein, s 294 of the *Telecommunications Act* preserves the exceptions in ch 4 of the *Interception Act*.

25 For their part, telecommunications service providers are required to develop procedures to ensure that the communications that are carried over their systems are capable of being intercepted and accessed, thus enabling them to comply with requests for access from national security and law enforcement agencies. These matters are addressed in ch 5 of the *Telecommunications (Interception and Access) Act 1979* (Cth) but are not considered in this article.

26 See, eg, Senate Standing Committee on Constitutional and Legal Affairs, *Interim Report on the Inquiry into the Security Legislation Amendment (Terrorism) Bill 2002 [No 2] and Related Bills* (2002); Ben Golder and George Williams, 'Balancing National Security and Human Rights:

Those who eschew the notion 'of balance as a metaphor for the relationship between security and liberty',[27] are likely to argue that to pit individual liberty against national security is to adopt a 'bi-polar notion of balance'[28] which is too simplistic, since it assumes that 'more of one necessarily means less of the other'[29], that is, that freedom and safety can be traded off on 'a sliding scale'.[30] They maintain that this safety/freedom notion is a misleading dichotomy which tends to conceal an irony, namely, that the pursuit of security in order to enhance the public interest in preventing, detecting and punishing terrorism and crime comes at the expense of protecting people's liberty from the state.[31] In fact, unchecked state interference can be just as damaging to individual liberty as terrorism and crime!

It has also been argued that the balancing rhetoric 'rarely achieves an accommodation between competing interests'.[32] In the context of the criminal justice system, Bronitt has stated that:

> In the relentless expansion of the powers of criminal investigation, suspects' rights are invariably 'traded off' against the community interests in preventing, detecting and prosecuting crime. Far from attaining the rhetoric of 'perfect equilibrium', the criminal justice system consistently favours the interests of the state over the individual.[33]

The same can be said of counter-terrorism legislation, including telecommunications interception powers. Legislative initiatives that are initially hailed as atypical responses to an unusual and critical situation (such as the threat of terrorism after 9/11 and the Bali bombings), over time, become normalised, and individual liberties are rarely restored to the level of protection they previously enjoyed.[34]

This paper does not proffer an opinion as to whether a balancing approach is the most appropriate means of reconciling the relationship between security and liberty. It simply proceeds on the assumption that individual privacy is an inevitable casualty of according national security and law enforcement agencies increased access to telecommunications information, and seeks to elucidate whether the intrusion on personal privacy under the telecommunications data regime is warranted.

Assessing the Legal Response of Common Law Nations to the Threat of Terrorism' (2006) 8 *Journal of Comparative Policy Analysis* 43. Of course there will be differences of opinion amongst these proponents as to how an appropriate balance should be struck.

27 Lucia Zedner, 'Securing Liberty in the Face of Terror: Reflections from Criminal Justice' (2005) 32 *Journal of Law and Society* 507, 508.

28 Ibid 532.

29 Ibid 511.

30 Philip Thomas, 'Emergency and Anti-Terrorist Powers 9/11: USA and UK' (2003) 26 *Fordham International Law Journal* 1193, 1208.

31 Zedner, above n 27, 532.

32 Simon Bronitt and James Stellios, 'Regulating Telecommunications Interception & Access: A Seachange in Surveillance Laws' in Katina Michael and M G Michael (eds) *Social Implications of Information Security Measures on Citizens and Business* (2006) 142.

33 Simon Bronitt, 'Electronic Surveillance, Human Rights and Criminal Justice' (1997) 3(2) *Australian Journal of Human Rights* 183, 185.

34 Thomas, above n 30, 1207–8.

THE ROLE OF PRIVACY IN SHAPING LAWS PERTAINING TO STATE ACCESS TO TELECOMMUNICATIONS INFORMATION

As a precursor to identifying how privacy concerns have shaped Australian telecommunications law, it is necessary to briefly recount the role that privacy has played in United States jurisprudence, as the latter has undoubtedly influenced the former.

Although 'privacy' is not explicitly mentioned in the Bill of Rights, courts have interpreted the Fourth Amendment to the United States Constitution as conferring an important privacy protection which has relevance to state access to telecommunications information. The Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized.

Early United States Supreme Court cases such as *Olmstead v United States*[35] gave a restricted interpretation to the concept of search and seizure, holding that it demands a physical trespass on property or a seizure of material goods. This meant that wiretapping was not caught or controlled by the Fourth Amendment in circumstances where the defendant's property or person was not touched. In 1967, in *Katz v United States,*[36] the Fourth Amendment was reinterpreted by the Supreme Court as an aspect of privacy. In that case, Katz was charged with transmitting betting information by telephone in violation of a federal statute. At Katz' trial, the government was permitted to introduce evidence of telephone conversations at Katz' end. These conversations were overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from which the calls were made. It was argued that the recordings had not been obtained in violation of the Fourth Amendment, since there was no physical entry into the area occupied by Katz. The Supreme Court overturned the narrow approach adopted in *Olmstead,* and held that the Fourth Amendment 'protects people not places'.[37] The Court permitted Katz to invoke the Fourth Amendment even though he was visible inside the booth, as he was not seeking to exclude the eye, but the uninvited ear, and was entitled to assume that the words he uttered in the telephone booth would not be broadcast to the world.[38]

The nub of the decision is that the reach of the Fourth Amendment no longer turns upon the presence or absence of a physical intrusion into a given enclosure; the Amendment was recast as a species of privacy, namely, the right to be let alone by an intrusive government.[39] Black J, in dissent, held that the words 'search and seizure'

---

35 277 US 438 (1928) ('*Olmstead*'). See also: *Goldman v United States,* 316 US 129 (1942); *On Lee v United States,* 343 US 747 (1952).

36 389 US 347 (1967).

37 Ibid (Stewart J).

38 Ibid 352 (Stewart J).

39 The perception of the Fourth Amendment as a species of privacy protection did not begin with the *Katz* case: Ken Gormley, 'One Hundred Years of Privacy' (1992) *Wisconsin Law Review* 1335. Rather, it has its roots in the case of *Boyd v United States*, 116 US 616 (1886) and the seminal article by Warren and Brandeis, in which privacy was famously described as 'the right to be let alone': Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193. Brandeis, who was a Harvard law professor at the time the article

simply could not be construed to cover eavesdropping carried on by electronic means, and castigated the majority for arbitrarily reinterpreting the Amendment as one based on privacy rather than one designed to protect citizens against unreasonable searches and seizures.[40] However, the concept of the 'reasonable expectation of privacy' enunciated by Harlan J[41] has endured, and is now firmly entrenched in Fourth Amendment jurisprudence, despite the fact that the word 'privacy' does not appear in the text of the Amendment.[42]

While Australians clearly do not enjoy the same entrenched constitutional protections against interference by the state as Americans, privacy is not entirely unrecognised. Australia is signatory to covenants that protect privacy, including Article 17 of the *International Covenant on Civil and Political Rights*, which provides that '[n]o one shall be subjected to arbitrary or unlawful interference with his privacy … or correspondence' and that '[e]veryone has the right to the protection of the law against such interference'. Common law and statute[43] also provide incidental protection of various aspects of privacy, and the common law appears to be progressing towards recognising a tort of privacy,[44] although the Australian Law Reform Commission has recommended that the Federal Parliament should introduce a statutory cause of action for a serious invasion of personal privacy rather than leave the courts to develop a privacy tort.[45]

Privacy initially played a prominent role in shaping laws governing state access to telecommunications. The first time that telephone interceptions was regulated in Australia by means of legislation was in 1960, when the *Telephonic Communications (Interception) Act 1960* (Cth) was enacted.[46] The Act made telephone interception an offence, then proceeded to carve out some very narrow exceptions in which interception could lawfully occur.[47] It is clear that the main object of the *Telephonic*

---

was published, was subsequently appointed to the United States Supreme Court. He sat on the *Olmstead* case, but dissented. However his dissenting judgment 'laid the groundwork for the constitutionalization of his notion of privacy': Ken Gormley, 'One Hundred Years of Privacy' (1992) *Wisconsin Law Review* 1335, 1357.

40 *Katz v United States*, 389 US 347, 364-374 (1967).

41 Ibid 361.

42 The Supreme Court of Canada has also adopted the notion of a reasonable expectation of privacy in interpreting s 8 of the *Canadian Charter of Rights and Freedoms,* which states that '[e]veryone has the right to be secure against unreasonable search or seizure': *Hunter (Director of Investigation and Research, Combines Investigation Branch) v Southam Inc* [1984] 2 SCR 145.

43 See, eg, the *Human Rights (Sexual Conduct) Act 1994* (Cth).

44 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199; *Grosse v Purvis* [2003] QDC 151; *Doe v ABC* [2007] VCC 281. But compare *Giller v Procopets* (2008) 40 Fam LR 378, which may have halted its progress.

45 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) 88 (Recommendation 74–1).

46 Before 1960, telecommunications interception was an executive act subject to prime ministerial directions which governed the exercise of executive power: Commonwealth, *Parliamentary Debates*, House of Representatives, 5 May 1960, 1423–4 (Sir Garfield Barwick, Acting Minister for External Affairs and Attorney-General); Thomas Wong, *Regulation of Interception of Communications in Selected Jurisdictions* (2005) 4.1.

47 For example, the *Telephonic Communications (Interception) Act 1960* (Cth) permitted interceptions to be carried out, with a warrant, for national security purposes, but not for

Communications (Interception) Act 1960 (Cth) was to protect the privacy of citizens in their communications, hence the sweeping prohibition and narrowly confined exceptions. When introducing the Bill into the House of Representatives, Sir Garfield Barwick, the Acting Minister for External Affairs and Attorney-General, stated:

> Eavesdropping is abhorrent to us as a people. Not one of us … would fail to recoil from the thought that a citizen's privacy could lightly be invaded … this Government has always been alive to these natural and proper reactions of our people. It has approached this question of permitting the interception of telephonic messages from that point of view.[48]

Undoubtedly the significant shift in US jurisprudence concerning the meaning of the Fourth Amendment was a contributing factor to the early pre-eminence of privacy in this context.

Since 1960, communications and surveillance technology have continued to burgeon. People now communicate in ways not previously possible; consequently, privacy can now be invaded in ways not previously possible. The legislation has undergone numerous modifications in an attempt to keep pace with technology. The 1960 Act was replaced by the *Telecommunications (Interception) Act 1979* (Cth), which was renamed the *Telecommunications (Interception and Access) Act 1979* (Cth) in 2006.[49] Advances in telecommunications technology have generated debate about the continuing role of privacy. Should the same level of privacy be afforded to all modern forms of communication as was afforded to landline telephone communications in 1960, when legislation was first introduced? Should individuals be expected to understand that when their mobile phone is switched on, there is an information flow between their phone and the cell towers, and to accept that a telecommunications service provider might be required to divulge this information to ASIO or to law enforcement agencies? Or should they have a reasonable expectation of privacy in respect of the information that is transmitted between phone and cell tower? The same issue arises in respect of Internet communications, which can be accessed more easily than real time communications as a result of the fact that they are temporarily stored on various computers during their transmission.[50]

The extent to which the federal government has been prepared to accommodate individual privacy in line with developments in communications technology varies according to the nature of the communication in question. The *Interception Act*

---

general law enforcement purposes. Subsequently, the *Telecommunications (Interception) Act 1979* (Cth) permitted interception as a means of investigating crime, but initially only in relation to serious narcotic offences.

48 Commonwealth, *Parliamentary Debates*, House of Representatives, 5 May 1960, 1423–4. See also *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222, 229; *R v Edelsten* (1990) 21 NSWLR 542, 549; *O'Malley v Keelty, Australian Federal Police Commissioner* (2004) FCA 1688, [2]; Bradley Holland, 'Overtaking Privacy in the Telecommunications Transit Lane' (2004) 11 *Privacy Law and Policy Reporter* 165.

49 The renaming of the *Telecommunications (Interception) Act 1979* (Cth) was effected by the *Telecommunications (Interception) Amendment Act 2006* (Cth).

50 Starey, above n 13, 28. These issues are currently being canvassed in the United States in the context of determining the extent to which individuals have a legitimate expectation of privacy under the Fourth Amendment: Daniel Sovocool and Kristin Jamerdino, 'Tracking a User's Location Via Cell Phone' (2006) ipfrontline.com <http://www.ipfrontline.com /depts /article.asp?id=9633&deptid=5> at 1 February 2009.

proceeds on the basis that there is a valid distinction between live communications and stored communications. The former are considered to be more deserving of privacy protection, as they are more spontaneous. By contrast, stored communications are more deliberative in that they provide the opportunity for 'second thoughts' prior to transmission; they therefore merit less privacy protection.[51] The upshot is that it is more difficult for a law enforcement agency to get a warrant to intercept a real time communication than it is to get a warrant to access a stored communication.[52] This dichotomy has not gone unchallenged.[53] Many are unconvinced by the notion that an email or an SMS message is a more considered form of communication than verbal comments made during a telephone call. As far as telecommunications data is concerned, the government's stance is that because this data does not consist of content, it deserves even less privacy protection, which is why it can be accessed under Chapter 4 without any warrant.

Although the extent to which privacy is protected varies according to the type of information in question, subsequent additions and modifications to the Act have invariably continued to identify the primary focus of the legislation as being to protect the privacy of communications.[54] Indeed, the Senate Legal and Constitutional Legislation Committee stated that the principal consideration of any legislation which governs access to personal communications should be the protection of privacy.[55] However, while lip service continues to be paid to privacy, the undoubted emphasis in the post 9/11 additions and amendments to the *Interception Act* has been on extending the circumstances in which national security and law enforcement agencies can access private communications.

Notwithstanding the pervasive threat of terrorism and the increased sophistication in criminal techniques, it is argued that the Australian Government as a responsibility to continue to protect the privacy of its citizens' communications. Indeed, the escalation in the volume and form of telecommunications information, coupled with the unremitting development of intrusive and sophisticated electronic surveillance devices and techniques, makes it not only imperative that privacy concerns continue to be accommodated in legislative regimes that facilitate access to telecommunications for national security and law enforcement purposes, but that they are restored to a place of primacy. Since there are 'no longer any technical barriers to the kind of Big Brother surveillance society envisioned by George Orwell', the *only* barriers that remain are

---

51 Blunn, above n 22, [1.4.2].

52 For example, stored communications warrants can be issued in relation to less serious criminal offences than interception warrants.

53 See, eg, Commonwealth, *Parliamentary Debates*, Senate, 28 March 2006, 85 (Senator Stott Despoja); Simon Bronitt and James Stellios, 'Regulating Telecommunications Interception and Access in the Twenty-First Century: Technological or Legal Revolution?' (2006) 24 *Prometheus* 413, 419.

54 See, eg, Explanatory Memorandum, Telecommunications (Interception) Amendment Bill 2006 (Cth) 9; Commonwealth Security Legislation Review Committee, Parliament of Australia, *Report of the Security Legislation Review Committee* (2006) 182; Australian Government, Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979, Annual Report for the Year Ending 30 June 2008* (2008) [2.2].

55 Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Provisions of the *Telecommunications (Interception) Amendment Bill 2006* (2006) [3.1]. A similar viewpoint was expressed in the Blunn Review: Blunn, above n 22, 5.

'political and legal'.[56] Accordingly, it behooves the legislature to cast national security and law enforcement exceptions in such a way as to minimise the intrusion on individual privacy. It will be argued that aspects of the telecommunications data regime encroach on individual privacy to an unacceptable extent. However, before analysing the regime, it is necessary to outline Part 13 of the *Telecommunications Act*, as the telecommunications data regime contained in Chapter 4 of the *Interception Act* operates as an exception to Part 13 and can only be understood in that light.

RESTRICTIONS ON THE DISCLOSURE AND USE OF INFORMATION BY TELECOMMUNICATIONS SERVICE PROVIDERS

Telecommunications service providers obtain a large range of information in the course of supplying telecommunications services to their customers, including details about subscriptions to telephone, Internet and other communications services.[57] They also carry, and in some instances store, the content of telecommunications.[58] Part 13 of the *Telecommunications Act* imposes an obligation on telecommunications service providers to protect the confidentiality of this information by prohibiting its disclosure or use.[59]

The primary disclosure and use offences are contained in Division 2 of Part 13. Section 276 provides that current and former 'eligible persons'[60] – defined as carriers,[61] CSPs,[62] telecommunications contractors[63] and their respective employees — must not disclose or use any information or document that relates to:

---

56 Barry Steinhardt, 'Liberty in the Age of Technology' (2004) *Global Agenda* 154, 154.

57 Australian Government, Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005) 49.

58 Ibid.

59 Part 13 is concerned only with the use and disclosure of information. It does not deal with other aspects of information handling, such as collection and storage: Australian Law Reform Commission, *Review of Australian Privacy Law,* Discussion Paper No 72 (2007) [63.144]. The handling of 'personal information' by telecommunications service providers is also subject to the *Privacy Act 1988* (Cth) ('the *Privacy Act*'): Australian Law Reform Commission, Report No 108, above n 45, [71.1]. The interaction between the *Privacy Act* and Part 13 of the *Telecommunications Act* is unclear, and has been considered in a number of reviews: see, for example: Australian Government, Office of the Privacy Commissioner, *Getting in on the Act*, above n 57, 49–63; Commonwealth, Senate Legal and Constitutional References Committee, Parliament of Australia, *The Real Big Brother: Inquiry into Privacy Act 1988* (2005) ch 4; Australian Law Reform Commission, *Review of Australian Privacy Law* Discussion Paper 72 (2007) ch 63; Australian Law Reform Commission, Report No 108, above n 45, ch 71. A discussion of the *Privacy Act* is beyond the scope of this paper.

60 *Telecommunications Act 1997* (Cth) s 271.

61 A carrier is the holder of a carrier licence granted under div 3 of pt 3 of the *Telecommunications Act*. A carrier licence must be held before certain infrastructure can be used to carry communications by means of guided and/or unguided electromagnetic energy: *Telecommunications Act 1997* (Cth) ss 7, 42, 56.

62 A carriage service provider is described as one who makes use of the infrastructure owned by a carrier to carry communications by means of guided and/or unguided electromagnetic energy: Australian Law Reform Commission, Report No 108, above n 45, [71.8]. Internet service providers are carriage service providers.

- the contents or substance of a communication that has been, or is being,[64] carried by a carrier or CSP;[65]
- carriage services supplied or intended to be supplied to another person by a carrier or CSP; or
- the affairs or personal particulars of another person, including any unlisted telephone number or address.

These prohibitions only apply to information or documents which have come to the person's knowledge or possession by virtue of the fact that they are an 'eligible person'.[66] A similar prohibition is imposed by ss 277 and 278 on current or former eligible number-database persons[67] and current or former emergency call persons respectively. Contravention of any of these provisions is an offence punishable on conviction by imprisonment for up to two years.[68] There are no civil penalty provisions.[69]

These sweeping prohibitions on disclosure and use are mitigated by a lengthy list of exceptions which are contained in Division 3 of Part 13. Although the primary exceptions pertaining to national security and law enforcement have been relocated in the *Interception Act*, two of the exceptions that remain in the *Telecommunications Act* also have relevance to these matters. The general prohibition on disclosure and use is expressed not to apply where information or a document is disclosed or used in connection with the operation of an enforcement agency[70] and is 'required or authorised under a warrant',[71] or, in any other case, where disclosure or use of

---

63 A telecommunications contractor is a person who performs services for or on behalf of a carrier or CSP, otherwise than in the capacity of an employee: *Telecommunications Act 1997* (Cth) s 274.

64 A communication that 'is being' carried includes a communication that has been collected or received by a carrier or CSP for carriage by it, but which has not been delivered by it: s 276(1)(a)(ii).

65 This prohibition only applies to a communication that is, or has been, carried by a carrier or CSP if the carriage was, is, or is proposed to be, delivered by means of guided and/or unguided electromagnetic energy: s 276(4).

66 Information or documents that do not come to a person's knowledge or possession in these circumstances are not within the purview of pt 13. However, if such information constitutes 'personal information', it may nevertheless be regulated under the *Privacy Act 1988* (Cth): Australian Law Reform Commission, Report No 108, above n 45, [71.19].

67 A number-database person includes number-database operators, number-database contractors and their employees. A number-database operator is a person in respect of whom a declaration is in force under s 472(1): *Telecommunications Act 1997* (Cth) s 272(1). Since there are currently no number-database operators, as no declaration is in force, this prohibition will not be explained in detail. See Australian Law Reform Commission, Report No 108, above n 45, [71.9].

68 *Telecommunications Act 1997* (Cth) ss 276(3), 277(3), 278(3). There have been no prosecutions for breaches of the prohibitions under Part 13 since the enactment of the *Telecommunications Act 1997* (Cth): Australian Law Reform Commission, Report No 108, above n 45, [71.84].

69 The Australian Law Reform Commission has recommended that civil penalties be introduced in addition to the criminal penalties: Australian Law Reform Commission, Report No 108, above n 45, [71.83]–[71.98].

70 The definition of an enforcement agency is dealt with below. See also *Telecommunications Act 1997* (Cth) s 280(2).

71 *Telecommunications Act 1997* (Cth) s 280(1)(a).

information or a document is 'required or authorised by or under law'.[72] It should also be noted that Part 14 of the *Telecommunications Act* continues to impose a general obligation on carriers and CSPs to do their best to prevent their telecommunications networks and facilities from being used to commit offences, and to give the authorities such help as is reasonably necessary for the purposes of enforcing the criminal law and laws which impose pecuniary penalties, protect the public revenue and safeguard national security.

The *Telecommunications Act* obliges telecommunications service providers to keep records of certain disclosures made under Part 13 and of disclosures made to enforcement agencies under Chapter 4 of the *Interception Act*, and to report annually to the Australian Communications and Media Authority ('ACMA') on the number of such disclosures.[73] Compliance with these requirements is monitored by the Privacy Commissioner.[74] In the 2005/06 year there were 944 367 reported disclosures.[75] This number rose to 1 165 391 in the 2006/07 year,[76] and decreased to 992 946 in the 2007/08 year.[77]

DISCLOSURE AND USE OF TELECOMMUNICATIONS DATA FOR NATIONAL SECURITY AND LAW ENFORCEMENT PURPOSES

As explained in the Introduction, Chapter 4 of the *Interception Act* is now the repository for the exceptions that permit telecommunications data to be disclosed or used for national security and law enforcement purposes. The exceptions are very significant. Of the 1 165 391 disclosures made by telecommunications service providers in the 2006/07 year, 845 012 – almost 73% — were made for the enforcement of the criminal law or a law imposing a pecuniary penalty or for the protection of public revenue;[78] in

72 *Telecommunications Act 1997* (Cth) s 280(1)(b). The disclosures and uses permitted under ch 4 are 'authorised' for the purposes of s 280. For the sake of clarity, the Australian Law Reform Commission has recommended that a note cross-referencing to ch 4 be inserted after s 280: Australian Law Reform Commission, Report No 108, above n 45, Recommendation 72–6.

73 *Telecommunications Act 1997* (Cth) pt 13 div 5. The reporting differs from that under the *Telecommunications (Interception and Access) Act 1979* (Cth), which is to Parliament.

74 *Telecommunications Act 1997* (Cth) s 309.

75 Australian Communications and Media Authority, *Annual Report 2005–06* (2006) Appendix 12.

76 Australian Communications and Media Authority, *Annual Report 2006–07* (2007) Appendix 12.

77 Australian Communications and Media Authority, *Annual Report 2007–08* (2008) Appendix 12. This figure includes disclosures made under the new ch 4. The ACMA Annual Report for the 2008/09 year does not contain statistics relating to the number of disclosures made by telecommunications service providers under the *Interception Act* for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of public revenue. Presumably, this is because ACMA is only required to include in its Annual Report statistics relating to information or documents that were disclosed under Division 3 of Part 13 of the *Telecommunications Act: Australian Communications and Media Authority Act 2005* (Cth) s 57(2)(f).

78 Australian Communications and Media Authority, *Annual Report 2006–07*, above n 76. These statistics do not include disclosures made to ASIO.

the 2007/08 year, 663 530 of the 992 946 disclosures were made for these purposes.[79] This paper will now outline those structural features of the regime that have the greatest impact on privacy. They are conveniently referred to as the 'what', 'who' and 'when' aspects of the regime.

Definition of 'telecommunications data' — what can be accessed under the regime?

Chapter 4 of the *Interception Act* governs access to 'telecommunications data' for national security and law enforcement purposes. One of the most controversial aspects of the scheme is definitional, namely, what constitutes 'telecommunications data'. The problem is that, although the Chapter is headed 'Access to telecommunications data', that phrase is not otherwise used in the Chapter, nor is it defined. The omission is surprising, given that the entire Chapter is devoted to the circumstances in which such data can be lawfully disclosed or used for national security and law enforcement purposes. The only assistance to be derived from the Act is to be found in ss 171 and 172. Section 171 makes it clear that telecommunications data consists of information or a document.[80] Section 172 operates negatively, by providing that Divisions 3 and 4 of Chapter 4 do not permit the disclosure of information or documents to the extent that they contain the contents or substance of a communication. The exclusion of 'contents or substance' is in deference to the other regimes under the *Interception Act* which require a person who wishes to gain access to such information for national security or law enforcement purposes to obtain an interception or stored communications warrant.[81] The upshot is that 'telecommunications data' is a shorthand description of what is left in respect of information or a document after the contents and substance of a communication have been removed.

When the Telecommunications (Interception and Access) Amendment Bill 2007 was remitted to the Senate Committee for inquiry and report, many of the submissions made to the Committee expressed concern at the Bill's failure to define the phrase or to specify what remains within the concept after 'contents and substance' are excised. Given that the entire scheme hinges on the meaning of this phrase, it has been convincingly argued that the Act creates 'unacceptable ambiguity and uncertainty about the "reach" of the various powers' that it confers on national security and law enforcement agencies.[82]

The Attorney-General's Department defended the status quo, arguing that any attempt to define 'telecommunications data' might be redundant in 12 months time.[83]

---

79 Australian Communications and Media Authority, *Annual Report 2007–08*, above n 77. These statistics do not include disclosures made to ASIO.

80 The Chapter describes itself as setting out circumstances where pt 13 does not prohibit a disclosure or use of information or a document: s 171(1), (2).

81 Explanatory Memorandum, Telecommunications (Interception and Access) Bill 2007 8. These regimes have been briefly described in the Introduction.

82 Australian Privacy Foundation, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007*, July 2007. A number of submissions to the Australian Law Reform Commission reference into privacy also argued that the phrase should be defined in the Act: Australian Law Reform Commission, Report No 108, above n 45, [73.30].

83 Evidence to Senate Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, Canberra, 16 July 2007, 22 (Catherine Smith) cited in Senate Standing Committee

The Senate Committee must have been convinced by this reasoning, as it did not recommend that the phrase be legislatively defined. The same position was adopted by the Australian Law Reform Commission ('ALRC') in its recent report on privacy on the basis that it is preferable to ensure that the legislation remains technology neutral so that it can apply to new technologies without the need for legislative amendment.[84] Only the dissenting report of the Australian Democrats recommended otherwise, arguing that the absence of a clear definition is not 'justified by an assertion that this will allow the law to remain current with technology'.[85] The fact that Parliament has seen fit to amend the *Interception Act* more than fifty times since its enactment in 1979 is testament to its readiness to revisit the legislation whenever the need arises. There is no reason why this cannot continue in relation to the meaning of 'telecommunications data'.

The Attorney-General's Department also expressed the belief that the relocation of the telecommunications data regime into the same Act as the interception and stored communications regimes would make it 'clearer when advising law enforcement and the carriers on what exactly is content and what is call associated data as new technologies come into place.'[86] With respect, the fact that these regimes are now housed in the one statute does not help to clarify the boundaries between them. Indeed, the Australian Privacy Foundation envisaged that the relocation of the national security and law enforcement exceptions would blur the distinction between interception legislation and the standard telecommunications legislation which controls access to other information such as customer details and traffic data, in a manner adverse to privacy.[87]

The upshot of the situation is that the only authoritative repository of information about the meaning of 'telecommunications data' is the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment Bill 2007.[88] The Explanatory Memorandum states that 'telecommunications data is available in relation to all forms of communications, including both fixed and mobile telephony services and for internet based applications including internet browsing and voice over internet telephony.'[89] Having loosely divided telecommunications into telephone based communications or Internet based telecommunications,[90] the Explanatory

on Legal and Constitutional Affairs, Parliament of Australia, *Telecommunications (Interception and Access) Amendment Bill 2007 [Provisions]* (2007) [3.17].

84 Australian Law Reform Commission, Report No 108, above n 45, [73.33].

85 Senate Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, *Telecommunications (Interception and Access) Amendment Bill 2007 [Provisions]: Minority Report by the Australian Democrats* (2007) [1.18].

86 Evidence to Senate Standing Committee on Legal and Constitutional Affairs, above n 83 [3.17].

87 Australian Privacy Foundation, above n 82.

88 *Acts Interpretation Act 1901* (Cth) s 15AB(2)(e).

89 Explanatory Memorandum, Telecommunications (Interception and Access) Bill 2007 (Cth) 6.

90 This distinction is becoming increasingly blurred as a result of 'IP telephony', which 'enables facsimile messages, video and other forms of data traditionally transmitted via the PSTN [('Public Switched Telephone Network')] to be transmitted via the internet': Australian Law Reform Commission, Report No 108, above n 45, [9.79]. Voice over the Internet Protocol services (VoIP), which enable verbal conversations to be conducted in real

Memorandum proceeds to state that 'telecommunications data' will vary according to the type of telecommunications service:

> For telephone-based communications, telecommunications data includes subscriber information, the telephone numbers of the parties involved, the time of the call and its duration.[91]

It then elaborates further:

> For fixed and mobile voice telephony, including voice calls, and voice- or text-messaging services, the term includes the details of the parties to the communication, the date, time and duration of the communication, the device used to send or receive the information, and (in some cases) the locations of the parties.[92]

In relation to Internet based applications 'telecommunications data includes the Internet Protocol (IP) address used for the session, the websites visited, and the start and finish time of each session.'[93] And later:

> For Internet based telecommunications, such as email, web browsing, instant messaging, or internet voice calls (Voice over Internet Protocol or VoIP), data includes the sender's and recipient/s' Internet addresses, the devices from which they were sent from or to, and the time and date at which it was sent. The information does not include content such as the subject line of an email, the message sent by email or instant message or the details of Internet sessions.[94]

Whilst there are clearly some non-controversial examples of telecommunications data — these include billing information, which records that a communication has occurred and includes details of the time and destination of phone calls made and received, the duration of the calls etc, and subscriber information, which includes details of the identity of the subscribers to a particular telecommunications service[95] — there are areas where the difference between 'telecommunications data' and the 'contents and substance' of communications remains difficult to decipher. In relation to telephone based communications, the main area of uncertainty is the status of mobile

---

time over the Internet, is a subset of IP telephony. The Australian Law Reform Commission notes that:

> VoIP services usually will be classified as carriage services for the purposes of the *Telecommunications Act 1997* (Cth). This means that VoIP service providers generally will be 'carriage service providers' that are required to observe the provisions in pt 13 of the *Telecommunications Act* that protect the confidentiality of telecommunications information: Australian Law Reform Commission, Report No 108, above n 45, [9.81].
>
> However, VoIP services can be isolated from the traditional PSTN, thereby allowing users to make and receive calls solely over the Internet. Examples given by the ALRC include instant messaging products such as Yahoo Messenger and MSN Messenger: Australian Law Reform Commission, Report No 108, above n 45, [71.101]. If a VoIP service does not connect with the PSTN at all, the service provider may not be regulated by the *Telecommunications Act,* although it might be regulated by the *Privacy Act:* Australian Law Reform Commission, Report No 108, above n 45, [9.81], [71.101].

91 Explanatory Memorandum, Telecommunications (Interception and Access) Bill 2007 (Cth) 6.

92 Ibid 8.

93 Ibid 6.

94 Ibid 8.

95 Australian Government, Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979, Annual Report for the Year Ending 30 June 2007* (2007) [3.13].

phone location data. In relation to Internet based communications, uncertainty surrounds the status of email message headers and details of Internet sessions. Each of these problem areas will be considered.

Mobile phone location data

It is important to establish whether mobile phone location information constitutes 'telecommunications data', since the location data provided by mobile phones is 'generated without any specific intervention' and its use 'for security and law enforcement purposes is obvious'.[96] Its potential impact on a person's privacy is equally self-evident.

Chapter 4 of the *Interception Act* is silent about the status of mobile phone location information. However, s 275A of the *Telecommunications Act* states that for the purposes of Part 13, information or a document about the location of a mobile telephone handset or other mobile communications device is taken to be information or a document 'that relates to the affairs of the customer responsible for the handset or device'. Since information or documents that relate to the affairs of a person are protected by Part 13, it must follow that when an exception to Part 13 is created – including the exceptions that are contained in the *Interception Act* – access to such information is permitted.[97] By virtue of s 275A, this would include location information. This appears to be the view adopted in the Explanatory Memorandum to the Telecommunications (Interception and Access) Bill 2007.[98] If information about the location of a person is regarded as 'telecommunications data', it can be disclosed to ASIO and law enforcement agencies without a warrant and without any independent oversight.[99] The impact and consequences of this assumed state of affairs on an individual's privacy are considered below.

Email message headers

Many of the submissions made to the Senate Committee stressed the need to resolve the confusion surrounding the status of email message headers. Emails have two parts: a body section and a header section. The body section contains the text of the message and is clearly content, and therefore outside the telecommunications data regime.[100] The header is divided into fields. The most common fields are the 'to and from' (or 'sender and recipient') email addresses, carbon copy (Cc or Bcc) addresses, the IP addresses, the subject line of the message, and the date it was written.[101] Uncertainty surrounds what parts of the header are properly regarded as 'telecommunications data'. While the Explanatory Memorandum states that email subject lines are not telecommunications data,[102] there is nothing explicit in the legislation to that effect

96 Blunn, above n 22, 1.1.25.

97 Electronic Frontiers Australia Inc, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007*, 10 July 2007 [3.2].

98 Explanatory Memorandum, Telecommunications (Interception and Access) Bill 2007 (Cth) 10, 13.

99 Electronic Frontiers Australia Inc, above n 97.

100 Access to the body section of an email would require a stored communications warrant.

101 Wikipedia, *E-mail* <http://en.wikipedia.org/wiki/E-mail> at 10 December 2008.

102 Explanatory Memorandum, Telecommunications (Interception and Access) Bill 2007 (Cth), 8. The same view is taken by the Attorney-General's Department: Australian Government,

and 'it cannot be known whether the same view would be held by all carriers and enforcement agencies.'[103] In the interests of protecting privacy and of preserving the integrity of the boundaries between the various access regimes established by the *Interception Act*, it is appropriate that national security and law enforcement agencies that seek to access the subject lines in email message headers should have to obtain a stored communications warrant, and that this should be made clear in the legislation.

Electronic Frontiers Australia ('EFA') noted a further problem with headers:

> email messages can carry significantly more other information in the header section than is equivalent to 'traffic information' associated with telephone calls. For example, some (probably most) email programs enable the end-user to create their own special header fields in outgoing messages, in which they can place any information they wish. These are often referred to as 'X' headers because, to ensure a user-defined name of a field will never conflict with standard header field names, they should be given field names commencing with 'X-'.[104]

EFA maintained that there is confusion as to whether this information is considered data or content, and argued that information made available to national security and law enforcement agencies under Chapter 4 in relation to emails should be limited to the sort of data that is available in respect of telephone calls, namely, traffic data. This would include dates, source and destination — that is, sender and receiver email address and IP address etc — but not the subject line or any other information contained in the header.

The Attorney-General's Department disputed EFA's claim that there is the capacity to include information in headers which are defined by the user:

> The EFA rely on an Internet Engineering Task Force (IETF) standard referred to as Request for Comment (RFC) 822. This is an obsolete standard that was superseded in 2001 by RFC 2822 and the relevant header fields stated by EFA cannot be found in the current standard. RFC 2822 also states that these obsolete fields 'MUST NOT be generated'.[105]

EFA subsequently conceded that Internet Standard RFC 822 had been rendered obsolete by Standard RFC 2822, but maintained that user–defined fields (X fields) continue to be allowed to be generated by RFC 2822. Consequently, the concern remains well founded.[106] If so, then in the interests of privacy and of maintaining clear boundaries between the various regimes, the legislation should specify which parts of a header constitute telecommunications data.

Attorney-General's Department, *Answers to Questions on Notice, Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007* Attorney- General's Department, 24 July 2007, Item 10, [11].

103 Electronic Frontiers Australia Inc, above n 97, [3.3].

104 Ibid.

105 Australian Government, Attorney-General's Department, *Answers to Questions on Notice,* above n 102, [12].

106 Electronic Frontiers Australia Inc, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007*, 26 July 2007, 2. EFA took the view that the phrase 'MUST NOT be generated' referred to obsolete syntax, not field names.

Internet sessions that involve web browsing

When a person browses the World Wide Web, the following details will always be generated: an Internet Protocol ('IP') address, a domain name and Uniform Resource Locators ('URLs'). An IP address is a number that identifies a computer that is connected to the Internet, and enables that device to locate other devices on the Internet.[107] An IP address has been likened to a telephone number, which identifies a particular telephone on a telephone network. A domain name is an alphanumeric, 'human-readable' equivalent of an IP address.[108] That is, they are names for host computers connected to the Internet.[109] Domain names are of no assistance to machines, which identify and communicate with each other using IP addresses. They are strictly used for human convenience.[110] Domain name servers transfer the human readable domain name into a machine readable IP address.[111] URLs are different again. Unlike domain names, URLs are designed to locate resources on the web. A URL is the address used to reach a document, page, file, image, website or other resource on the world wide web. It is made up of a number of parts. The first part is a protocol identifier, which tells the web browser what sort of server it will be communicating with in order to fetch the file/ page/ resource.[112] The next component of a URL is the domain name.[113] There might also be a path which indicates where the web page is located within the web space of the website, that is, within that computer. Paths take the user to files, folders and sub-directories.

The issue that arises is whether the details that are generated when a person engages in a web browsing Internet session can be appropriately described as 'telecommunications data'.[114] Chapter 4 of the *Interception Act* is silent about the status of such details. To make matters worse, the Explanatory Memorandum contains contradictory statements about which details of an Internet session are properly regarded as telecommunications data. The quotes reproduced earlier reveal that at one point, telecommunications data is said to include 'the Internet Protocol (IP) address used for the session, the websites visited and the start and finish time of each session', but later, telecommunications data pertaining to Internet based communications is said not to include the details of Internet sessions.

---

107 IP addresses are 32 bit numbers expressed in four octets. Lindsay explains that
[t]he IP address has two main parts: the network prefix (or network address), which identifies the network a computer is attached to; and the host ID (or host address), which identifies the logical location of the host computer on the network: David Lindsay, *International Domain Name Law: ICANN and the UDRP* (2007) 5.

108 Ibid 6.

109 Ibid 4.

110 Marshall Brain, *How Domain Name Servers Work* (2000) HowStuffWorks.com <http://www.howstuffworks.com /dns.htm> at 2 February 2009.

111 Ibid. See also Webopedia.com *Domain Name* <http://www.webopedia.com/TERM/D/domain_name.html> at 2 February 2009.

112 Boutell.com, *WWW FAQs: What is a URL?* (2003) <http://www.boutell.com/newfaq/definitions/url.html> at 1 February 2009. The most common protocol is the hypertext transfer protocol ('http') which is the protocol used to transfer web pages.

113 The protocol identifier and the domain name are separated by a colon and two forward slashes.

114 If not captured as 'telecommunications data', access to information regarding Internet sessions would be permitted only under a stored communications warrant.

While there is a general consensus that the Explanatory Memorandum is ambiguous and needs to be clarified, the submissions made to the Senate Committee reveal strong disagreement as to which details of Internet sessions are correctly characterised as telecommunications data. The disagreement centres on the extent to which the data that is captured in an Internet session is qualitatively different from data about telephone calls and email messages.

The Attorney-General's Department argued that IP addresses should be regarded as telecommunications data since they do not reveal in anything but the most general terms the nature of the communication or the activity of the individual at that site:

> In relation to getting call-associated data regarding an IP address that can identify a web page, that is not content because all it does is tell a law enforcement agency that a certain target went to a certain website. It does not tell them any other details. It does not tell them that they then went into their bookings on line or via their travel agent or that they downloaded particular information. It does not give them any knowledge of the substance as to why they were on that web page. URLs are a little different because they will then point out the continuum of where the person actually went to.[115]

The Attorney-General's Department likened access to an IP address to the knowledge gained from a phone number. For example, a telephone call to the switchboard of a large organisation shows the caller's interest in that organisation but will not reveal which extension within the PABX system the caller was connected to.[116] Similarly, an IP address only indicates that an individual visited a specific Internet page; it does not indicate the activities occurring when that site was visited. In relation to URLs the following comments were made:

> With regard to web URLs … and how an apparatus finds that on the internet, I will go back to the analogy of when we used to make telephone calls; if we had call charge records we would have a list of numbers that a person called but it does not show content. It is the same reason with the URL. It would have a web server log with a list of URLs and by that nature it does not show content, it just shows a list of URLs. If an officer wants to phone those numbers and find out what they are they could ring them systematically. It is the same with a computer. When they go and click that button to search that URL, it is the same thing. The request is done automatically from that PC to a domain name server or system to find that URL over the Internet. But it does not actually look at content.[117]

EFA took a different view. Firstly, it maintained that web site and web page addresses can provide information about the content of a communication; indeed, it can be as revealing as an email subject line. Therefore, as a matter of parity, and in the interests of technological neutrality, if the subject lines of emails should be excluded from the concept of 'telecommunications data', so should web page addresses. EFA also argued that once details of web pages visited are obtained by a national security or law enforcement agency, this is likely to provide the agency with access to the actual

---

115 Evidence to Senate Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, Canberra, 16 July 2007, 31 (Catherine Smith) cited in, Senate Standing Committee on Legal and Constitutional Affairs, *Telecommunications (Interception and Access) Amendment Bill 2007 [Provisions]* (2007) [3.18].

116 Australian Government, Attorney-General's Department, *Answers to Questions on Notice*, above n 102, [18].

117 Evidence to Senate Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, Canberra, 16 July 2007, 42 (Lionel Wayne Markey).

content that was communicated to the person. Of course, if historical Internet content is being accessed, the content that is retrieved may not be identical to that which was accessed by the target at an earlier point in time. However, as EFA pointed out, it is often possible to go to a web archive to find actual content as at a past date.[118] In relation to prospective information supplied in near real time, 'the probability that enforcement agencies will be able to access, at the provided web page address, the actual content communicated to the person is vastly increased.'[119]

Unlike the Attorney-General's Department, EFA took the view that access to web browsing activity is qualitatively different to access to telephone call data, being more privacy invasive:

> It is akin to filming individuals' activities in a manner that records every item they purchase in shops, every film they see at the cinema or hire or buy, every book and magazine they glance through and/or purchase or take out on loan from a library and so on.[120]

Similar comments were made by the Australian Privacy Foundation.[121] It is argued that this view more closely approximates the true nature of what is being accessed, and that accordingly, web page addresses and details of web pages visited should be treated as content, not as telecommunications data. This should be made clear in the legislation.

These three problem areas do not exhaust the definitional issues that are capable of arising. The ALRC has recently conceded that stakeholders need a clearer understanding of what is encompassed by the term 'telecommunications data'. It recommended that this clarity be provided via guidelines issued by the Attorney-General's Department, rather than by legislative definition.[122] However, definitional issues should be addressed in the legislation that establishes the scheme; the provision of guidance should not be relegated to a government department which may have a stake in the outcome, particularly if national security is involved.

Nicholls and Rowland make the concerning point that in the absence of a defined meaning, law enforcement agencies themselves are likely to shape the meaning of the phrase.[123] They explain that these agencies 'represent an epistemic community', meaning that they 'discuss issues with each other and created [sic] a consensus view which relates to all of the agencies' needs.'[124] The authors anticipate that this phenomenon creates a danger that the meaning of 'telecommunications data' will evolve rapidly, resulting in an 'environment where the metadata delivered is determined by the agencies'.[125] This has obvious implications for individual privacy.

---

118 Electronic Frontiers Australia Inc, above n 97, [3.4].
119 Ibid.
120 Ibid.
121 Australian Privacy Foundation, above n 82.
122 Australian Law Reform Commission, Report No 108, above n 45, [73.35]. The ALRC Report noted that the Attorney-General's Department maintains that it already 'provides guidance to agencies and carriers regarding these issues, both generally and on a case-by-case basis': [73.32].
123 Rob Nicholls and Michelle Rowland, 'Regulating the Use of Telecommunications Location Data by Australian Law Enforcement Agencies' (2008) 32 *Criminal Law Journal* 343, 349.
124 Ibid.
125 Ibid.

WHO CAN ACCESS TELECOMMUNICATIONS DATA UNDER THE REGIME?

Chapter 4 contemplates that telecommunications data can be disclosed to ASIO and to enforcement agencies. An 'enforcement agency' is defined as:

- the Australian Federal Police;
- a State police force or service;
- the Australian Commission for Law Enforcement Integrity;
- the Australian Crime Commission;
- the New South Wales Crime Commission;
- the Independent Commission Against Corruption of New South Wales;
- the Police Integrity Commission of New South Wales;
- the Office of Police Integrity in Victoria;
- the Crime and Misconduct Commission of Queensland;
- the Corruption and Crime Commission of Western Australia;
- an authority established by or under a law of the Commonwealth, State or Territory that is prescribed by the regulations to be an enforcement agency;
- a body or organisation responsible to the Ministerial Council for Police and Emergency Management-Police;
- the CrimTrac Agency; or
- any body whose functions include administering a law which imposes a pecuniary penalty or which relates to the protection of the public revenue.[126]

There is cause for concern about some of the organisations that are included in this definition. The first area of controversy pertains to paragraph (k) of the definition, which allows for additions and expansions to the list by regulation. In its submission to the Senate Committee, the Law Council of Australia objected to the fact that the Executive is empowered to expand the definition, noting that no justification had been proffered as to why the efficient operation of the *Interception Act* requires the Executive to have this degree of flexibility.[127] The Attorney-General's Department sought to justify the inclusion of the power, arguing that it will allow agencies to be included whenever their investigative functions change to the extent that access to telecommunications data becomes necessary.[128] In 2008, the Australian Customs Service was added to the definition of an enforcement agency pursuant to this provision[129]

A second area of controversy relates to the inclusion of CrimTrac in the list. CrimTrac was established in 2000 by agreement between the Commonwealth, States

126 *Telecommunications (Interception and Access) Act 1979* (Cth) s 5.

127 Law Council of Australia, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007*, July 2007, 13.

128 Australian Government, Attorney-General's Department, *Answers to Questions on Notice*, above n 102, [10].

129 *Telecommunications (Interception and Access) Amendment Regulations 2008 (No 1)* (Cth).

and Territories.[130] It describes itself as an agency that 'assists Australian police services to take advantages of the opportunities opened up by forensic science, information technology and communications advances.'[131] It aims to generate national approaches to law enforcement techniques and information sharing solutions by delivering national database systems such as a National Child Sex Offender Register, a National Automated Fingerprint Identification System and a National Criminal Investigation DNA Database. The objection to the inclusion of CrimTrac in the list is that it is neither a criminal law enforcement agency, nor an agency that conducts investigations into suspected offences.[132] Rather, it is in the nature of a service agency that provides databases for a number of enforcement agencies.[133] Given that it does not perform investigatory or enforcement functions, there appears to be no justification for empowering it to issue authorisations for access to telecommunications data.[134]

The Attorney-General's Department appealed to the fact that the inclusion of CrimTrac is not new, but is simply a transfer from the *Telecommunications Act*, and that until it is established that it is inappropriate to include CrimTrac, it should remain on the list. With respect, this does not address the aforementioned concerns. Moreover, it is the inclusion of an agency that should be justified, not its exclusion.

The Senate Committee, having considered the submissions and the response of the Attorney-General's Department, recommended that CrimTrac be removed from the definition of enforcement agency. The Committee maintained that in light of the intrusive nature of the authorisation powers, the default position should be that an agency should not be included unless there is a positive justification for doing so.[135] However, the recommendation was not implemented, and CrimTrac remains on the list.

A final area of controversy pertains to the inclusion on the list of any body whose functions include administering a law which imposes a pecuniary penalty or which relates to the protection of the public revenue. This would include bodies such as the Australian Tax Office, the Australian Securities and Investment Commission and similar State and Territory agencies. The main concern is the change in wording of this provision during its transition from the *Telecommunications Act* to the *Interception Act*. Under the former Act, only agencies that were 'responsible for' administering a law

130 This agency is underpinned by an Inter-Governmental Agreement signed by all Australian police ministers to establish and operate CrimTrac. The Intergovernment Agreement is reproduced in Appendix Three of the first annual report of CrimTrac: CrimTrac Agency Annual Report 2000-01.

131 CrimTrac, *About Us* (2008) <http://www.crimtrac.gov.au/about_us/index.html> at 2 February 2009.

132 Senate Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, *Telecommunications (Interception and Access) Amendment Bill 2007 [Provisions]* (2007) [3.6]. There is also a concern that CrimTrac's inclusion in the list would enable it to access stored communications: [3.6].

133 Australian Privacy Foundation, above n 82, 5.

134 Expunging CrimTrac from the definition does not necessarily mean that it could never be privy to telecommunications data. This would depend on whether such data could be deposited in its databases by other agencies making a permissible use of the secondary use provisions, which are discussed below.

135 The Dissenting Report issued by the Australian Democrats also recommended that CrimTrac be removed from the definition: Australian Democrats, above n 85, [1.13].

imposing a pecuniary penalty or a law relating to the protection of public revenue were included in the definition. Now, such agencies need only have functions that 'include' administering such laws. It has been observed that a body can have functions that 'include' administering such laws, without necessarily being 'responsible' for their administration.[136] The extent to which the addition of bodies to the list is as a result of this change of wording is unclear. In light of this uncertainty, it would be preferable to identify these agencies by name and to justify their inclusion.[137]

Given the significant powers that are reposed in enforcement agencies under Chapter 4 and their impact on privacy, the definition of an 'enforcement agency' should be narrowly circumscribed, and certainly should not be a matter for conjecture.

WHEN CAN TELECOMMUNICATIONS DATA BE ACCESSED UNDER THE REGIME?

This section will critically analyse the precise circumstances in which telecommunications data – whatever that phrase may mean — can be accessed by ASIO and enforcement agencies for national security and law enforcement purposes. Divisions 3 and 4 of Chapter 4 of the *Interception Act* set out the circumstances in which ss 276, 277 and 278 of the *Telecommunications Act* do not prohibit the *disclosure* of telecommunications data — whether in the form of information or a document — for national security or law enforcement purposes. Division 5 sets out the circumstances in which these provisions do not prohibit the *use* of such data.

Chapter 4 makes provision for two types of permitted disclosure: voluntary disclosure and authorised disclosure. Both the voluntary and authorised disclosure provisions contemplate that telecommunications data can be lawfully disclosed to ASIO and 'enforcement agencies'. In respect of authorised disclosure, a distinction is drawn between data that is in existence at the time of the request — that is, historical data — and prospective data. More stringent restrictions are imposed on access to the latter.

VOLUNTARY DISCLOSURE

Sections 276, 277, and 278 of the *Telecommunications Act* do not prohibit the voluntary disclosure by a person of information or a document to ASIO if the disclosure is in connection with the performance of ASIO's functions.[138] In similar vein, information and documents can be disclosed to an enforcement agency if the disclosure is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue.[139] The person making the disclosure would be one of the persons referred to in ss 276, 277 and 278, most likely a carrier or CSP. The voluntary disclosure provisions do not apply if the Director-General of Security, the Deputy-Director of Security or an officer or employee

136 Electronic Frontiers Australia Inc, above n 97, [5.2.2(b)].
137 See, eg, Australian Privacy Foundation, above n 82, 5.
138 *Telecommunications (Interception and Access) Act 1979* (Cth) s 174(1).
139 *Telecommunications (Interception and Access) Act 1979* (Cth) s 177(1), (2).

of ASIO, or, in the case of an enforcement agency, a 'relevant staff member',[140] requests the holder to disclose the information or document, since other provisions deal with the disclosure of information pursuant to an authorisation.[141] The requirement that voluntary disclosures must be unsolicited is intended to prevent agencies from pressuring carriers into supplying them with information rather than utilising the authorisation process.[142]

The voluntary disclosure provisions cater to the situation where an employee of a carrier or CSP encounters information in the course of his or her duties that the employee regards as being 'in connection with' ASIO's functions or 'reasonably necessary' for the enforcement of the criminal law etc. It permits the disclosure to be made, notwithstanding that a request has not emanated from those bodies. The ALRC observed that the provision creates difficulties for employees who do not believe they are in a position to make an effective judgment as to whether a disclosure is 'in connection with …' or 'reasonably necessary for ...'.[143] It also creates the possibility of oversupply, meaning that an employee might disclose more information than is necessary for ASIO and enforcement agencies to perform their functions.[144] This has implications for privacy. However, despite these risks, it is not advocated that provision for voluntary disclosure be removed, as it is important that carriers and CSPs who come across vital information be free to divulge it. Rather, it is preferable to limit the risk of oversupply, and the consequent intrusion on privacy, by means of controls. Suggestions as to how this can be achieved include: a proposal by the Australian Democrats that there should be a positive obligation on ASIO and enforcement agencies to warn employees that they are not legally obliged to make voluntary disclosures;[145] a recommendation in the Blunn Review that the provisions be reviewed with a view to clarifying the objective and better identifying the process to be followed;[146] and a recommendation by the ALRC that the Attorney-General's Department develop guidelines as to the circumstances in which voluntary disclosure is permitted.[147]

Authorised disclosure of existing information or documents

Notwithstanding ss 276, 277, and 278 of the *Telecommunications Act*, certain persons within ASIO and the enforcement agencies are empowered to authorise telecommunications service providers to disclose specified information or documents

---

140 A relevant staff member of an enforcement agency is the head or deputy head of the agency, or any employee, member of staff or officer of the agency: *Telecommunications (Interception and Access) Act 1979* (Cth) s 5.

141 *Telecommunications (Interception and Access) Act 1979* (Cth) s 174(2), 177(3).

142 Australian Privacy Foundation, above n 82, 4.

143 Australian Law Reform Commission, Discussion Paper No 72, above n 59, [63.50]. The observation was made in respect of the voluntary disclosure provisions as they then appeared in the *Telecommunications Act*.

144 This is particularly true of ASIO, whose functions are listed in very general terms. For example, one of its functions is 'to obtain, correlate and evaluate intelligence relevant to security': *Australian Security Intelligence Organisation 1979* (Cth) s 17(1)(a).

145 Australian Democrats, above n 85, [1.39].

146 Blunn, above n 22, [1.7.6].

147 Australian Law Reform Commission, Report No 108, above n 45, [73.78]–[73.79].

that were in existence at the time the person from whom the disclosure is sought received notification of the authorisation.

In the case of ASIO, the persons who can make such authorisations are the Director-General of Security, the Deputy Director-General of Security, or an officer or employee of the Organisation who has been approved in writing by the Director-General to authorise disclosures to be made.[148] Before a disclosure can be authorised, the authorising person must be satisfied that the disclosure would be 'in connection with' the performance by the Organisation of its functions.[149] These functions are set out in the *Australian Security Intelligence Organisation Act 1979* (Cth).[150]

In the case of an enforcement agency, an 'authorised officer' may authorise the disclosure of specified information or documents only if he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue.[151] Although there is no express nexus with the agency's functions, this is probably implicit in the reasonable necessity requirement. The phrase 'reasonably necessary' appears to impose a higher threshold than the 'in connection with' that is required before a disclosure to ASIO can be authorised. Presumably this reflects a view that a lower threshold is appropriate in cases involving national security. An authorised officer of an enforcement agency is defined as the incumbent or acting head or deputy head of the agency, or a person who holds or is acting in a particular management position or office in the agency that has been designated by the head of the agency as an authorised officer.[152]

The requirement that the authorising officer merely be 'satisfied' that a disclosure would be 'in connection with …' or 'reasonably necessary for …' has attracted criticism. The Queensland Council for Civil Liberties noted that the legislation fails to specify precise criteria that would entitle the authorising officer to be satisfied that the disclosure would be in connection with the performance of ASIO's functions.[153] This omission enables the authorising person to give the broadest interpretation to ASIO's functions. The same point can be made in relation to enforcement agencies. This state of affairs makes it practically impossible for a person whose telecommunications data is or was sought by ASIO or an enforcement agency to contest the disclosure.[154]

---

148 *Telecommunications (Interception and Access) Act 1979* (Cth) s 175(2).

149 *Telecommunications (Interception and Access) Act 1979* (Cth) s 175(3).

150 *Australian Security Intelligence Organisation Act 1979* (Cth) s 17.

151 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 178(3), 179(3). Note that in relation to the enforcement of a law imposing a pecuniary penalty or protecting public revenue, it is only ss 276 and 277 of the *Telecommunications Act 1997* (Cth) that are expressed not to prevent a disclosure, not s 278: *Telecommunications (Interception and Access) Act 1979* (Cth) s 179(1).

152 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 5 (definition of 'authorised officer'), 5AB. The definition is designed to reflect the differing management structures of enforcement agencies: Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) 3.

153 Queensland Council for Civil Liberties, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007*, 10 July 2007, 2.

154 New South Wales Council for Civil Liberties, above n 1, 2.

Authorised disclosure of prospective information or documents

Separate provision is made for the disclosure of prospective information on an ongoing basis. Despite the description of the information as 'prospective', in reality, the information would be delivered or streamed to ASIO or an agency in near real time. It is prospective only in the sense that it is not in existence at the time the authorisation is made. The information might consist of information about a person's Web browsing activities,[155] or might concern the real time location of a phone or device.[156] The need to differentiate between historical and prospective data is justified in the Explanatory Memorandum as 'a reflection of the advances in technology, which enables the use of telecommunications data to provide location information'.[157] A prospective authorisation is qualitatively different from a request to produce information that is already kept as part of the provider's operational system. It is essentially a request to the carriers and CSPs to 'proactively monitor their customers and intentionally store every piece of information they are able to store'.[158] In deference to the higher privacy implications of accessing prospective data, more restrictive access conditions are imposed. This section of the paper will describe the prospective information regime, consider the adequacy of the in-built privacy protections, and offer suggestions as to how the current regime might be improved. Ultimately, it will be argued that the privacy protections do not meet the objections to the scheme, and that in view of the fact that access to prospective data is more akin to real time interception and surveillance,[159] rather than traffic data in the customary sense of the word, access to such data should be procured via a warrant.

Authorised disclosure to ASIO

Sections 276, 277 and 278 of the *Telecommunications Act* are expressed not to prohibit the disclosure of prospective information or documents if the disclosure is covered by an authorisation.[160] Due to the greater privacy implications involved in accessing prospective data, an authorisation can be issued only by the Director-General of Security, the Deputy Director-General of Security or certain other high ranking officers or employees of the Organisation.[161] The authorisation can sanction the disclosure of specified information or documents that come into existence during the period for which the authorisation is in force, provided the authorising person is satisfied that the disclosure would be in connection with the performance of the Organisation's

---

155 The extent to which details generated by Web browsing constitute telecommunications data was considered in an earlier section of this article.

156 Electronic Frontiers Australia Inc, above n 97, [3.2], [5.4].

157 Explanatory Memorandum, Telecommunications (Interception and Access) Bill 2007 (Cth) 10.

158 Evidence to Senate Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, Canberra, 16 July 2007, 13 (Irene Graham).

159 Ibid.

160 *Telecommunications (Interception and Access) Act 1979* (Cth) s 176(1).

161 They must be officers or employees who hold or are acting in a position that is equivalent to, or higher than, an SES (Senior Executive Service) Band 2 position in the Department: *Telecommunications (Interception and Access) Act 1979* (Cth) s 176(2). These persons are the Organisation's senior management and leadership: Australian Law Reform Commission, Report No 108, above n 45, [73.16].

functions.[162] An authorisation comes into force when the person from whom the disclosure is sought is notified of its existence, and ends at the time specified in the authorisation, which must be no longer than 90 days from the day it was made, unless it is revoked earlier.[163] An authorisation must be revoked if it is no longer required,[164] which would be the case if the reasons for granting it no longer existed. The authorisation can also sanction the disclosure of information or documents that were already in existence before the authorisation came into force, thereby avoiding the need for a separate authorisation to be made for access to historical data.[165]

In a submission to the Senate Committee, the Inspector-General of Intelligence and Security ('IGIS') proposed that his office should have a role in examining authorisations by ASIO to access prospective telecommunications data.[166] IGIS is an independent statutory position created by the *Inspector-General of Intelligence and Security Act 1986* (Cth) which reviews a number of security agencies, including ASIO, to ensure that they are held accountable for their compliance with the law, the propriety of their activities and their respect for human rights.[167] In discharging these duties, IGIS is empowered to conduct inspection activities.[168] The Inspector-General proposed that as part of his office's inspection program, he should examine requests for access to prospective data to ensure that there is sufficient justification for the authorisations and that any procedural requirements imposed by the Communications Access Co-ordinator are met.[169] The Senate Committee agreed, and recommended that the Inspector-General incorporate such oversight into his regular inspection program.[170]

Authorised disclosure to enforcement agencies

Prospective information can be lawfully disclosed pursuant to an authorisation made by an authorised officer of a criminal law-enforcement agency.[171] A criminal law-enforcement agency includes all the agencies that come within the definition of enforcement agency except: a body or organisation responsible to the Ministerial Council for Police and Emergency Management-Police; the CrimTrac Agency; or any

162 *Telecommunications (Interception and Access) Act 1979* (Cth) s 176(4).
163 *Telecommunications (Interception and Access) Act 1979* (Cth) s 176(5).
164 *Telecommunications (Interception and Access) Act 1979* (Cth) s 176(6).
165 *Telecommunications (Interception and Access) Act 1979* (Cth) s 176(3).
166 Inspector-General of Intelligence and Security, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007*, 11 July 2007, [10].
167 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 4. The Inspector-General also reviews the Australian Secret Intelligence Service, the Defence Intelligence Organisation, the Defence Imagery and Geospatial Organisation, the Defence Signals Directorate and the Office of National Assessments.
168 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 9A.
169 The provenance of these procedural requirements is explained below.
170 Senate Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, *Telecommunications (Interception and Access) Amendment Bill 2007 [Provisions]* (2007) [3.79]. The Senate Committee took the view (on advice from the Attorney-General's Department) that IGIS already has jurisdiction to oversee ASIO's use of its power to obtain prospective telecommunications data under s 8(1) of its establishing Act and that accordingly, legislative amendment was not necessary to enable this to occur: [3.67].
171 *Telecommunications (Interception and Access) Act 1979* (Cth) s 180(2).

body whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue.[172] The more restrictive control over who may authorise the disclosure of prospective information is said to be a concession to the greater privacy implications involved in accessing such data. An authorisation can be made in respect of specified information or documents that come into existence during the period for which the authorisation is in force.[173] An authorisation comes into force when the person from whom the disclosure is sought is notified of it, and ends no more than 45 days from when it is made, unless it is revoked earlier, which must be done if disclosure is no longer required.[174]

Prospective authorisations cannot be issued unless the authorised officer is satisfied that disclosure is reasonably necessary for the investigation of an offence against a law of the Commonwealth, State or Territory that is punishable by imprisonment for at least three years.[175] Moreover, before the authorisation is made, the authorised officer must have regard to the extent to which the privacy of any person(s) would be likely to be interfered with by the disclosure.[176] Interestingly, the same requirement is not imposed on ASIO officers seeking access to prospective data, although the IGIS would be well placed to make an assessment of the regard had to privacy by authorised officers of ASIO as part of his inspection program. This is the only occasion in Chapter 4 in which interference with privacy is expressly required to be taken into account. Given that the stated primary raison d'etre of the *Interception Act* is to protect privacy, it is unclear why privacy is not required to be taken into account in respect of all authorisations.

The legislation does not specify how this responsibility pertaining to privacy must be fulfilled. It was suggested to the Senate Committee that there ought to be explicit legislative guidance as to how this obligation should be discharged.[177] The Attorney-General's Department disagreed, claiming that privacy considerations 'will vary enormously according to the unique circumstances of each situation', and 'may include the relationship between the seriousness of the offences being investigated, the value of the information likely to be obtained, and the extent to which accessing this information would, in the circumstances, breach an individual's privacy'.[178] The Explanatory Memorandum suggests that having regard to privacy would involve an assessment of the value of the information sought, compared with the privacy of the user(s) of the telecommunications service(s) in question.[179] The *Telecommunications*

172 *Telecommunications (Interception and Access) Act 1979* (Cth) s 5.

173 As is the case with ASIO, the authorising person can also authorise the disclosure of specified historical information or documents, thereby avoiding the need for a separate application to be made for access to historical data: *Telecommunications (Interception and Access) Act 1979* (Cth) s 180(3).

174 *Telecommunications (Interception and Access) Act 1979* (Cth) s 180(6), (7).

175 *Telecommunications (Interception and Access) Act 1979* (Cth) s 180(4).

176 *Telecommunications (Interception and Access) Act 1979* (Cth) s 180(5).

177 See, eg, Office of the Privacy Commissioner, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007*, July 2007, [3.2].

178 Australian Government, Attorney-General's Department, *Answers to Questions on Notice*, above n 102, [4].

179 Explanatory Memorandum, Telecommunications (Interception and Access) Bill 2007 (Cth) 13.

(Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2007, which lays down procedural requirements relating to authorisations, requires an authorisation of this nature to include a statement that the authorised officer 'had regard to how much the privacy of any person(s) would be likely to be interfered with by the disclosure and is satisfied that the impact on privacy is outweighed by the seriousness of the conduct being investigated'. This requirement imposes an obligation on the authorising officer to conduct a balancing process between privacy and the expected benefits to the criminal investigation in question. However, it does not require the authorising officer's 'satisfaction' to be based on reasonable grounds; nor does it contain a list of specific factors that must be taken into account in the process of reaching a conclusion. Without these, the process can be easily reduced to one of box ticking.[180] Accordingly, it is argued that a set of specific criteria should be included in the legislation to which the authorising officer must have regard and must document.

THE MOBILE PHONE AS TRACKING DEVICE – USING THE TELECOMMUNICATIONS DATA REGIME FOR SURVEILLANCE PURPOSES

Although the *Interception Act* imposes stricter controls over access to prospective information in light of the greater encroachment on privacy, these controls do not counteract all the problems inherent in the prospective authorisation scheme. As far as telephone based communications are concerned, the prospective data most likely to be sought will be the location information generated by a mobile phone.[181] The dangers associated with this in terms of its impact on privacy will now be considered. However, before doing so, it should be noted that other objections can be raised to the prospective data regime. While these will not be considered in this paper, two are worthy of mention. First, there is a concern that the access scheme for prospective telecommunications data weakens the protection conferred by the *Surveillance Devices Act 2004* (Cth) and the *Australian Security Intelligence Organisation Act 1979* (Cth). Second, it has been suggested that a CSP may not be able to give effect to prospective information authorisations in relation to email traffic information without engaging in unlawful interception.

The tracking technologies

Technology is constantly improving the accuracy of the mobile phone as a tracking device. As location technologies become increasingly accurate, the greater will be their potential to track an individual's activities not just their general location. The implications for that individual's privacy are self-evident. Not surprisingly, there is considerable disquiet about the appropriateness of a scheme which facilitates access to such information without a warrant or any other form of rigorous, independent oversight. Currently, there are several technologies that can be used to determine the position of a particular mobile phone user. They include cell identification and GPS.

---

180 The New South Wales Council for Civil Liberties described it as 'lip service' that 'could use some teeth': New South Wales Council for Civil Liberties, above n 1, 2.

181 The discussion in this section proceeds on the assumption that location information is 'telecommunications data'. This issue has been explored earlier in this article.

The cell identification system relies on the cellular signal emitted by the mobile phone and picked up by the mobile phone towers to compute the position of the phone.[182] This signal passes from cell to cell as the phone moves from place to place whenever the phone is switched on, not just when the user is engaged in a call. This technology 'calculate[s] mobile location from network available information.'[183] The cell identification system has its shortcomings. For example, it only gives an approximate location, since it can only track people to towers. Accordingly, the larger a cell area, the less accurate the location information. Moreover, the signal can be easily interrupted by hills and buildings. However, despite its limitations, this system has proven successful for law enforcement purposes. Notable examples include the minor speeding offence that turned into serious criminal charges against former Federal Court judge Marcus Einfeld[184] and the trial of Ian Huntley for the murder of two girls in Soham in the United Kingdom.[185]

The other main tracking technology is 'built in GPS', which is a global positioning system built into the mobile phone itself. It is a handset based geo-location technology which is becoming a standard feature in most new mobile phones.[186] Like an ordinary mobile phone, a GPS receiver relies on radio waves, but instead of using towers on the ground it communicates with a network of 26 satellites that orbit the earth.[187] To

---

182 The location of a phone can be determined in a number of ways, based on the measurements of the signal. These include the signal's angle of approach to the cell towers, how long it takes the signal to travel to multiple towers and the strength of the signal when it reaches the towers: Tracy Wilson, *How GPS Phones Work* (2009) HowStuffWorks.com <http://electronics.howstuffworks.com/gps-phone.htm> at 2 February 2009. These various methods are explained in greater detail in: Australian Government, Australian Communications Authority, *Location Location Location: The Future Use of Location Information to Enhance the Handling of Emergency Mobile Phone Calls* (2004) 27–32. This report can be viewed at <http://www.acma.gov.au/webwr/consumer_info/location.pdf>.

183 Australian Communications Authority, *Location Location Location*, above n 182, 27.

184 Marcus Einfeld's mobile phone records suggested that he had lied under oath when he said that he was not in Sydney at the time the driving offence was committed and that his car was being driven by a friend. The records demonstrated that he was making calls from his mobile phone in the area where the car was caught speeding. He has since pleaded guilty to one count of perjury and one count of acting to pervert the course of justice: Janet Fife-Yeomans, 'Former Judge Marcus Einfeld Admits Lie, Has Cancer', *Daily Telegraph* (Sydney), 31 October 2008; James Madden, 'Guilty Marcus Einfeld Faces Jail as Prosecutors Push for Prison Sentence' *The Australian* (Sydney), 1 November 2008.

185 An automatic electronic 'goodbye' from a phone belonging to one of the girls as it was turned off showed that the girls could be traced to a spot outside the home of Ian Huntley, who was ultimately convicted of their murders. Mobile phone records also helped to destroy an alibi given by Huntley's ex-girlfriend, who said that she was with him at the time of the murders: BBC, *Soham trial: crucial phone evidence* (2003) <http://news.bbc.co.uk/2/hi/uk_news/england/cambridgeshire/3246111.stm> at 13 December 2008.

186 Australian Government, Australian Communications Authority, *Location, Location, Location*, above n 182, 7.

187 These satellites are established and operated by the United States Department of Defence: ibid 32. The European Union is currently building a global navigation satellite system called the Galileo System as an alternative to the US Global Positioning System. The system is expected to be operational by 2013. Unlike the US system which is under military

determine a phone's location, a GPS receiver has to determine the locations of at least three satellites above the phone and where the phone is in relation to those satellites.[188] Using trilateration, the receiver can determine the phone's location to within a few metres, based on the time it takes for signals to get to and from the satellites.[189] Once the handset has calculated its own position, the calculation is sent to the network.[190]

A phone with a standalone GPS receiver can struggle to lock on to the GPS satellite signal in a central business district or inside a building, and can take several minutes to establish a location fix, especially when the phone is first switched on.[191] Assisted GPS is designed to address this problem. Assisted GPS is the name given to a system whereby an outside source (an assistance server), on request, helps the GPS receiver inside the phone to establish a location fix.[192] The assistance server has vastly superior computing power than the built in GPS receiver, and boosts the performance of what the receiver could do on its own, both in terms of the time needed to determine a location using GPS and the accuracy of the mobile phone location information.[193] To communicate with an assistance server, the mobile phone must be able to access the Internet, as the assistance server is on the Internet. The assistance data goes from the Internet to the cellular network to the mobile phone. Assisted GPS is therefore a combination of network based and handset based location solutions.

The objections

Assuming location information constitutes 'telecommunications data', ASIO and criminal law-enforcement agencies are likely to authorise access to such information held by telecommunications service providers under the Chapter 4 regime. Many of the submissions to the Senate Committee argued that access to prospective mobile telephone data should be subject to more stringent control than mere authorisation by officers in ASIO or a criminal law-enforcement agency, albeit that the authorised

---

control, the Galileo system will be under civilian control: Thomas D'Roza and George Bilchev, 'An Overview of Location-Based Services' (2003) 21(1) *BT Technology Journal* 20.

188 Wilson, above n 182.

189 The handsets do not transmit any information to the satellites; thus the satellites are not cognisant of individual receivers or aware that a user's location is being calculated: Australian Government, Australian Communications Authority, *Location Location Location*, above n 182, 33.

190 Ibid 27. Note, however, that Waters has stated that there is 'no evidence that this detailed location information (generated by mobile phones incorporating GPS technology) is routinely accessible to the telco providing the service': Nigel Waters, *Government Surveillance in Australia* (2006) 23 <http://home.iprimus.com.au/nigelwaters/Government%20Surveillance%20in%20Australia%20v6.pdf> at 2 February 2009.

191 Australian Government, Australian Communications Authority, *Location Location Location*, above n 182, 33; *Assisted GPS (A-GPS) Powering the Real World Web* (2006) GPS Technology Reviews <http://gpstekreviews.com/2006/12/01/assisted-gps-a-gps-powering-the-real-world-web/> at 2 February 2009.

192 Australian Government, Australian Government, Australian Communications Authority, *Location Location Location*, above n 182, 33.

193 Jimmy LaMance, Jani Janvinen and Javier DeSalas, *Assisted GPS: A Low-Infrastructure Approach* (2002) GPS World <http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=12287> at 2 February 2009.

officers are high ranking ones. Of particular concern is the fact that a mobile phone that a person carries voluntarily can be used to track that person without the law enforcement agency having to go to the trouble of covertly installing a tracking device on the person's property or body. The dissenting report of the Australian Democrats stated that

> a person's mobile telephone ... should not be used as a surrogate tracking and tracing technology for people in the absence of any countervailing public interest, significant independent oversight and public reporting.[194]

The Democrats recommended that a warrant should be required for access to location information. In similar vein, EFA argued that

> a warrant should be required similar to the existing surveillance device warrants in the Commonwealth and the various states, or with similar conditions attached as the stored communications warrants.[195]

The Attorney-General's Department responded to these arguments by appealing to the fact that the power to access location information was already extant under the *Telecommunications Act*; the only difference is that Chapter 4 explicitly acknowledges that the sought after telecommunications data can be historical or prospective. As regards prospective data, the Department argued that the concerns about the heightened invasion of privacy are allayed by the more stringent controls on access outlined earlier, namely, the tighter limits on the agencies that can access prospective information, the stricter time limitations and the restriction to more serious offences. However, this does not meet the objections outlined above. In light of the fact that prospective location information is tantamount to surveillance, access to it should be procured only via a warrant, and, as is the case with the interception and stored communications regimes, in deciding whether to issue a warrant, the issuing authority should be required to have regard to the degree to which the privacy of a person would be interfered with.

USE OF TELECOMMUNICATIONS DATA CONNECTED WITH PROVISION OF ACCESS

Division 5 provides that ss 276, 277 and 278 of the *Telecommunications Act* 1997 do not prohibit information or a document from being *used* by a person — as distinct from being *disclosed* — provided that, by reason of Division 3 (access to telecommunications data by ASIO) or Division 4 (access to telecommunications data by enforcement agencies), the disclosure of the information or document by the telecommunications service provider was lawful, and the use is for the purposes of, or connected with, the lawful disclosure.[196]

Secondary disclosure and use of telecommunications data

The primary disclosure and use provisions regulate the disclosure of information by telecommunications providers to ASIO or enforcement agencies, and control the use to

---

194 Senate Standing Committee on Legal and Constitutional Affairs, *Minority Report by the Australian Democrats*, above n 85, [1.24].

195 Evidence to Senate Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, Canberra, 16 July 2007, 12 (Irene Graham).

196 *Telecommunications (Interception and Access) Act 1979* (Cth) s 181.

which that information can be put by the recipient agency. In contrast, Division 6 focuses on secondary disclosure and use, that is, on the subsequent disclosure and use of telecommunications data that has been lawfully obtained by ASIO or an enforcement agency under the primary disclosure provisions.[197] Can such information be passed on to other bodies by the recipient of the primary disclosure and used by them?

Information disclosed to enforcement agencies

It is an offence for an enforcement agency to use or disclose telecommunications data it has received by reason of a lawful disclosure.[198] However, this general prohibition on the secondary use and disclosure of information by enforcement agencies is qualified by a number of exceptions. The prohibition is expressed not to apply to disclosures to ASIO where the disclosure is reasonably necessary for the performance by ASIO of its functions.[199] Nor does it apply to disclosures or uses that are reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of public revenue.[200] For example, if, during an investigation into a taxation fraud, the Australian Taxation Office obtains telecommunications data that concerns drug trafficking, the Australian Taxation Office could lawfully disclose this information to a relevant police agency to investigate.[201] This concession is significant, as it means that the information can be used in a different investigation from that for which it was initially sought.

There is disagreement as to whether these lawful secondary disclosures are effectively limited to situations where the agency receiving the secondary disclosure could have obtained the information directly from the carrier or CSP under the primary disclosure rules. The view of the then Attorney-General is that secondary disclosures can be made only to agencies that could have accessed the information directly from the telecommunication provider under the primary disclosure rules.[202] Thus the provisions are justifiable because all they are doing is permitting agencies to give information to another agency in circumstances where the recipient agency could have accessed the information itself, the advantage being that the recipient agency may not have been aware that the information existed or, if it did become aware, it may no longer exist on the carrier's network.[203] By contrast, EFA argues that, at least in

197 The Act does not deal with third and subsequent disclosure or use.

198 *Telecommunications (Interception and Access) Act 1979* (Cth) s 182(1). The penalty for breach is imprisonment for 2 years.

199 *Telecommunications (Interception and Access) Act 1979* (Cth) s 182 (2)(a).

200 *Telecommunications (Interception and Access) Act 1979* (Cth) s 182(2)(b)–(d), 182(3).

201 Explanatory Memorandum, Telecommunications (Interception and Access) Bill 2007 (Cth) 14.

202 Letter from Attorney-General The Hon Philip Ruddock to Mr Burgess, Chief Executive Officer, Police Federation of Australia, 07/2852. This letter is attached to: Police Federation of Australia, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007,* 9 July 2007. See also Australian Government, Attorney-General's Department, *Answers to Questions on Notice*, above n 102, [14].

203 Australian Government, Attorney-General's Department, *Answers to Questions on Notice*, above n 102, [14].

relation to prospective information, the secondary disclosures are not subject to the same limitations as primary disclosures and gives the following example:

> In relation to criminal law-enforcement agencies, s 182(2) permits secondary disclosure and use of 'prospective' information for purposes for which the information could not have been disclosed/obtained in the first place, i.e. secondary disclosure/use in relation to investigation of offences with a penalty of less than 3 years. The authorisation of initial/primary disclosure of prospective information is restricted to when reasonably necessary for the investigation of an offence that is punishable by imprisonment for at least 3 years and before making the authorisation the authorised officer must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.[204]

EFA argued that s 182(2) should be amended to prohibit secondary disclosure and use of information except under the same conditions as primary disclosure and use.

The Law Council of Australia identified another anomaly in the secondary disclosure and use provisions as regards authorisations for access to prospective information. It is clear that Chapter 4 does not permit agencies such as the Australian Taxation Office to issue authorisations for access to prospective information as they are not criminal law-enforcement agencies. Nor can such authorisations be issued for the purpose of enforcing a law that imposes a pecuniary remedy or the protection of public revenue, as they can be made only for the investigation of serious criminal offences. These protections would be meaningless if the information can be shared amongst these agencies by way of a secondary disclosure for a variety of purposes. Yet the Law Council maintains that s 182 allows such sharing to legally occur. It recommended that s 182 be amended to prevent criminal law-enforcement agencies from disclosing prospective information to an agency that cannot itself authorise access to prospective information or from disclosing prospective information for a purpose which is not itself capable of providing grounds for such an authorisation.[205]

Information disclosed to ASIO

The *Interception Act* does not prohibit the secondary disclosure and use of information that has been lawfully disclosed to ASIO under Division 3. At first blush, the consequence appears to be that ASIO is free to disclose information — including prospective telecommunications data — to any person for any purpose, including secondary disclosures to agencies that are not empowered by Chapter 4 to access that information directly from carriers and CSPs.[206] However, the communication of intelligence information by ASIO officers, employees and contractors is regulated by the *Australian Security Intelligence Organisation Act 1979* (Cth). That Act imposes a general obligation of secrecy, but outlines a number of circumstances in which information can be lawfully disclosed to other authorities.[207]

---

204 Electronic Frontiers Australia Inc, above n 97, [5.6].
205 Law Council of Australia, above n 127, 9.
206 Electronic Frontiers Australia Inc, above n 97, [5.6].
207 *Australian Security and Intelligence Organisation Act 1979* (Cth) ss 18, 19.

OPERATIONAL ASPECTS OF THE TELECOMMUNICATIONS DATA REGIME: PROCESS, OVERSIGHT AND ACCOUNTABILITY

Up to now, this paper has focussed on the boundaries of the telecommunications data regime — the 'what', 'who' and 'when' questions. Other objections to the scheme pertain not to its scope, but to its operational aspects.

Responsibility for formulating requirements for the procedural aspects of authorisations, notifications of authorisations and revocations of authorisations is reposed in the Communications Access Co-ordinator ('CAC'), which is a statutory position created by the *Interception Act*.[208] The CAC is empowered under Chapter 4 to determine these requirements following consultation with ACMA and the Privacy Commissioner.[209] The requirements are contained in the *Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2007*. For the most part, the Determination simply specifies the information that must be included in authorisations, notifications and revocations[210] and provides that they must be signed by their maker.[211]

The main objection to the process is that insufficient provision is made for oversight 'before the event', that is, before the telecommunications data is disclosed. Oversight cannot be entrusted to the individuals whose telecommunications data is targeted, as they are unlikely to be aware that ASIO or enforcement agencies are seeking access to their data. Accordingly, they are not in a position to take steps to ensure that their privacy is adequately respected and the legislation is complied with. An independent entity is therefore needed to ensure that the scheme operates properly and according to law. However, no 'voice' is built in to the authorisation process system which can speak or act on behalf of individuals whose data is sought to be accessed.[212] Too much is left to the good faith of the agencies.

The fact that no warrant is required to access telecommunications data means that there is no involvement or oversight in the authorisation process by members of the judiciary or the AAT. This is to be compared with the interception and stored communications regimes, where a warrant is required.[213] While it might be justifiable to dispense with the need for a warrant for access to historical telecommunications data on the basis that it does not involve content and consists of what has traditionally been regarded as traffic data, it is not appropriate to permit access to prospective data

---

208 *Telecommunications (Interception and Access) Act 1979* (Cth) s 6R. The position is currently filled by the First Assistant Secretary, National Security Law and Policy Division in the Australian Government Attorney-General's Department: *Telecommunications (Interception and Access) (Communications Access Coordinator) Specification 2009* (Cth).

209 *Telecommunications (Interception and Access) Act 1979* (Cth) s 183.

210 They include the identity of the eligible person making the authorisation and proof of their eligibility, the relevant provision of the Act under which authorisation is sought, details of the information or documents to be disclosed, the date on which the authorisation was made etc.

211 If notifications or revocations of authorisations are in electronic form, it is sufficient if they state a unique identifier of the Organisation or agency.

212 It appears that some oversight will be exercised by the IGIS, but only at the behest of their own initiative.

213 But note that warrants issued to ASIO are issued by the Federal Attorney-General and, in some cases, by the Director-General of Security, not by members of the judiciary or AAT.

on the authorisation of a public servant. In this respect, the scheme appears to be beset by a lack of parity with the interception and stored access regimes. It has also been observed that this approach sets Australia apart from the United States and European countries, where a warrant is required for access to location based information.[214] However, it should be conceded that the warrant regime that applies to interception and stored communications has its own problems. First, very few Federal Court judges have agreed to be nominated as eligible judges.[215] Their hesitancy appears to be attributable to *Grollo v Palmer*,[216] in which the High Court held that the power to issue warrants is not part of the judicial power of the Commonwealth, but an exercise of executive power. Although the High Court proceeded to hold that judges could undertake this function in their personal capacity provided certain conditions were fulfilled,[217] judges have been reluctant to be nominated. Accordingly, the vast majority of warrants are issued by members of the AAT rather than by members of the judiciary.[218] Second the statistics reveal that when an interception or stored communications warrant is sought, it is almost never refused, thus indicating that law enforcement and national security considerations will almost always trump privacy concerns.[219] This led Bronitt and Stellios to claim that the warrant system that governs interceptions and access to stored communications is not necessarily an 'effective bulwark against the arbitrary intrusion into privacy'.[220]

One way in which concerns about the interests of individuals might be addressed is by introducing an independent Public Interest Monitor ('PIM') into the regime, such as exists in Queensland under the *Police Powers and Responsibilities Act 2000*.[221] Under that Act, the role of the PIM is to monitor applications for, and the use of, (inter alia) surveillance device warrants, retrieval warrants and covert search warrants.[222] In particular, the PIM monitors compliance by police officers with the requirements pertaining to applications for warrants and appears at any hearings of an application to a judge or magistrate for a warrant to test the validity of the application by presenting questions for the applicant to answer, by examining or cross examining any witnesses and by making submissions on the appropriateness of granting the

214 Nicholls and Rowland, above n 123, 350.

215 Only nine Federal Court judges and 12 Family Court judges have made themselves available, compared with 34 Federal Magistrates and 37 AAT members: Australian Government, Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979, Annual Report 2008*, above n 54, Table 42.

216 (1995) 184 CLR 348.

217 The judge must consent to the conferral of the non-judicial function and the non-judicial function must not be incompatible with the judge's judicial functions.

218 During the 2007/08 year, 90.72% of telecommunications interception warrants were issued by AAT members, 5.85% by Family Court Judges, 3.14% by Federal Magistrates and 0.22% by Federal Court Judges: Australian Government, Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979, Annual Report 2008*, above n 54, [4.71].

219 During the 2007/08 year, 3254 applications were made for interception warrants. 3246 were granted and only eight were refused or withdrawn. In the same year, all 117 applications for stored communications warrants were granted: ibid Table 1, Table 47.

220 Bronitt and Stellios, in Michael and Michael (eds), above n 32, 146. For further observations about the warrant system see Bronitt and Stellios, 'Telecommunications Interception in Australia', above n 3, 882.

221 See also *Crime and Misconduct Act 2001*(Qld).

222 *Police Powers and Responsibilities Act 2000* (Qld) s 740.

application.[223] The PIM also gathers statistical information on the use and effectiveness of the warrants, and makes annual reports to the Minister.[224]

In their Supplementary Report on the *Telecommunications (Interception and Access) Amendment Bill 2007* (Cth), the Australian Democrats recommended that the Queensland PIM model should be incorporated into the telecommunications data regime. The Democrats perceived that a PIM would act as an independent umpire who would 'balance necessary, lawful, and proportionate access by law enforcement agencies to telecommunications data with the public's right to communicate free from surveillance'.[225] The suggestion has merit, irrespective of whether a warrant system is introduced. Under the current system, the PIM could have a consultation role with agencies before they apply for an authorisation for historical or prospective data, or, in the event that a warrant system is introduced for access to prospective data, the PIM could be permitted to appear whenever an application for such a warrant is made to an issuing authority in order to question the applicant, cross examine any witnesses and make submissions to the issuing authority. The Democrats' recommendations for a warrant system for prospective telecommunications data and/or for the appointment of a PIM were not adopted by the government when the draft legislation was being considered.

The telecommunications data regime contains certain provisions that are designed to secure accountability 'after the event'. For example, the heads of enforcement agencies are required to retain authorisations for historical and prospective information for a period of three years[226] and must report annually to the Minister on the number of authorisations made.[227] No such reporting requirements are imposed on ASIO under Chapter 4.[228] The Minister must prepare a report that contains the information set out in each report made by the head of the enforcement agency, and must table this report in Parliament.[229] None of these reports can enable a person to be identified,[230] which is entirely appropriate given that they ultimately become a matter of public record.

Certain criticisms can be made of these 'back end' accountability measures.[231] Firstly, Chapter 4 does not require the destruction of records where the information

---

223 *Police Powers and Responsibilities Act 2000* (Qld) s 742.

224 *Police Powers and Responsibilities Act 2000* (Qld) ss 742(2)(e), 743.

225 Senate Standing Committee on Legal and Constitutional Affairs, *Minority Report by the Australian Democrats*, above n 85, [1.32].

226 *Telecommunications (Interception and Access) Act 1979* (Cth) s 185.

227 *Telecommunications (Interception and Access) Act 1979* (Cth) s 186(1). The report must break down the authorisations into the various categories: the number of authorisations for access to existing information or documents for the enforcement of the criminal law, for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue and, for criminal law-enforcement agencies, the number of authorisations for access to prospective information or documents.

228 ASIO is subject to certain reporting requirements under s 94 of the *Australian Security Intelligence Organisation Act 1979* but they do not relate to authorisations under ch 4 of the *Interception Act*.

229 *Telecommunications (Interception and Access) Act 1979* (Cth) s 186(2), (3).

230 *Telecommunications (Interception and Access) Act 1979* (Cth) s 186(4).

231 This phrase is coined by Bronitt and Stellios 'Telecommunications Interception in Australia' above n 3, 886.

obtained pursuant to an authorisation is irrelevant or is no longer likely to be required for a permitted purpose. This is to be compared with the situation that exists in relation to interceptions and stored communications, where destruction of records is required in certain circumstances.[232] While it might be argued that the primary use provision in s 181 creates an equivalent protection, since it effectively prohibits the use of data that is not relevant to an investigation, making a destruction requirement unnecessary, in the interests of privacy, and in order to achieve parity with the interception and stored communications regimes, such information should be required to be destroyed.[233] The problem with this recommendation is that an agency can conclude that information provided to it pursuant to an authorisation is not relevant to an investigation only if the question is considered and a view is formed. Accordingly, there is a need for a complementary requirement that there be a regular review of information.[234]

Secondly, enforcement agencies need only report annually to the Minister on the *number* of authorisations made during that year.[235] The reports are not required to contain any details of the authorisations, although the Minister is able to request that a report set out 'any other matter'.[236] Nor are they required to include details of secondary disclosures; hence there are no statistics on the extent to which telecommunications data is passed on. Moreover, the regime does not confer on anyone an inspection role in relation to authorisations.[237] This is in contrast to the interception and stored communications regimes, where the Commonwealth Ombudsman is given a large degree of oversight. In relation to interceptions, the Commonwealth Ombudsman is required to inspect the records of interceptions that must be kept by Commonwealth agencies in order to ascertain the extent to which these agencies have complied with obligations pertaining to record destruction and the keeping of records and documents connected with the issue of interception warrants. The Ombudsman must report the results of the inspection to the Minister on an annual basis.[238] Because the record keeping requirements imposed on the agencies are so detailed, an inspection is likely to reveal any deficiencies in procedure. The Ombudsman's report must include particulars of any such deficiencies that impact on the integrity of the telecommunications interception regime and particulars of any remedial action, if any, taken or proposed to be taken to address those deficiencies.[239] Inspections that expose any other breaches of the *Interception Act* can also be the subject

232 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 79, 150.

233 See also Australian Law Reform Commission, Report No 108, above n 45, [73.98]–[73.103].

234 See Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006) [3.74]–[3.81] for a recommendation to this effect in relation to the stored communications regime.

235 As explained, the Minister, in turn, reports to Parliament: *Telecommunications (Interception and Access) Act 1979* (Cth) s 186(2).

236 *Telecommunications (Interception and Access) Act 1979* (Cth) s 186(1)(d). It should be noted that telecommunications service providers are obliged to keep records of authorisations: *Telecommunications Act 1997* (Cth) pt 13 div 5.

237 The Communications Access Co-ordinator is given a role in scoping the form of authorisations, notifications of authorisations and revocation of authorisations (see s 183) but this is not an inspection role.

238 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 83–92A. These record keeping and record destruction obligations are imposed on agencies by ss 79–81.

239 *Telecommunications (Interception and Access) Act 1979* (Cth) s 84(1A).

of a report.[240] Similar inspections and reports must be made in respect of stored communications in order to ascertain, so far as is practicable, the extent of compliance with the record keeping and destruction requirements.[241] The relevant State or Territory Ombudsman generally undertakes this function for State and Territory agencies.[242] To ensure parity, consideration should be given to whether the Ombudsman should be given a similar role over the telecommunications data regime.

CONCLUSION

This paper has examined the telecommunications data regime contained in Chapter 4 of the *Interception Act*. Overall, the greatest objection to the regime pertains to its impact on privacy, particularly in relation to prospective data. In light of the fact that prospective data includes location data, the regime essentially sanctions surveillance of an individual's movements. This is a far cry from the traditional notion of telecommunications data as basic traffic information. While to date, the use of the prospective data regime has been minimal,[243] the potential exists for criminal law-enforcement agencies to make increased use of these powers in the future.

As it currently stands, the Chapter 4 regime errs on the side of liberality rather than caution in facilitating access to telecommunications data. Suggestions have been made throughout this paper as to how the regime could be reconfigured to accord more protection to privacy. Many of these suggestions advocate tightening the scope of the boundaries of the regime — the 'what', 'who' and 'when' questions. Suggestions have also been made as to how the operational aspects of the scheme should be reconfigured so that an independent voice either oversees the operation of the regime, or at least represents the interests of individuals whose data is sought to be accessed.

240 *Telecommunications (Interception and Access) Act 1979* (Cth) s 85.

241 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 152–8. These record keeping and record destruction obligations are imposed on agencies by ss 150, 151. They are less onerous than the record keeping requirements imposed in respect of interceptions.

242 This is not true in all cases. Inspection of the South Australian Police is undertaken by the Police Complaints Authority (South Australia), not by the State Ombudsman, while inspections of the Victoria Police and the Office of Police Integrity are undertaken by the Special Investigations Monitor (Victoria): Australian Government, Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979, Annual Report 2008*, above n 54.

243 In the period from 1 November 2007 to 30 June 2008, only 1,135 disclosures of prospective information were made to criminal law-enforcement agencies, compared with 289,745 disclosures of existing information for the enforcement of the criminal law and 88,144 disclosures of existing information for the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue: Australian Government, Australian Communications and Media Authority, *Annual Report 2007–08*, above n 77, Appendix 12, Disclosures of Information.

Calls for a review of the operation of the regime have come from a number of sources, including the Senate Committee[244] and the ALRC.[245] It is to be hoped that a review does eventuate, and that full consideration is given to the need to amend the regime to restore an appropriate level of personal privacy.

244 The Senate Committee recommended 'that the Attorney-General's Department arrange for an independent review of the operation of the *Telecommunications (Interception and Access) Act 1979* within five years': Senate Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, *Telecommunications (Interception and Access) Amendment Bill 2007 [Provisions]* (2007) [3.80].

245 The ALRC recommended that the *Telecommunications Act* and the *Interception Act* be reviewed to consider whether they continue to be effective in light of changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. In particular, it called for a consideration of whether the *Interception Act* should provide for a PIM to oversee interception and access of communications before interception or access takes place, although in making this recommendation, the ALRC was not only concerned with the Chapter 4 regime: Australian Law Reform Commission, Report No 108, above n 45, [71.61]–[71.71], Recommendation 71–2.