CHAPTER 3

STORED COMMUNICATIONS

Introduction

3.1 The principal consideration of legislation which governs access to personal communications should be the protection of privacy. However, it is accepted that in limited circumstances it may be in the public interest to allow access to such communications. It is therefore essential that any legislation permitting access to personal communications achieves an appropriate balance between preserving privacy and assisting law enforcement agencies to effectively investigate serious offences. The primary test must always be whether the seriousness of the offence being investigated sufficiently warrants a significant invasion of an individual's privacy. This is particularly important whenever access to information is by covert interception.

3.2 The proposed amendments create a general prohibition on access to stored communications subject to prescribed exceptions including a stored communications warrant. The effect of the general prohibition proposed in this Bill is to prevent law enforcement agencies from serving notices to produce to obtain stored communications from a carrier without the knowledge of the intended recipient.

3.3 The proposed amendments clarify the lawful position surrounding access to stored communications which has previously been under dispute. This includes the ability of enforcement agencies to use warrants pursuant to section 3L of the *Crimes Act*, or other lawful notices to produce, to covertly obtain stored communications.

3.4 Generally, the clarification of access to stored communications provided by the Bill has been welcomed as a necessary and significant improvement. However, a number of areas of concern regarding the proposed stored communications warrants, as well as some definitional issues have emerged in the submissions and evidence received by the Committee at the hearing. These issues are considered in the following sections.

Access to stored communications

3.5 Section 108 prohibits access to stored communications 'without the knowledge of the intended recipient of the stored communication.'[1] The Explanatory Memorandum states that:

> The requirement for knowledge also preserves the ability of law enforcement agencies to access stored communications held by a carrier where they do so with the knowledge of the intended recipient … The distinction means that enforcement agencies are regulated by the stored

1 Proposed subsection 108(1)(b)

> communications regime only when they are acting covertly in the access to these communications.[2]

3.6 Electronic Frontiers Australia (EFA) argue that enforcement agencies should not be permitted to use existing notices to produce at the carrier because 'there is no means by which the carrier can know whether or not the intended recipient has in fact been notified by the agency prior to disclosing the information.'[3]

3.7 EFA also suggest that there is a lack of clarity in the existing telecommunications legislation, in particular the interrelationship between the *Telecommunication (Interception) Act 1979* and the *Telecommunications Act 1997* regarding the authorisation of agencies to obtain the content of stored communications via compulsory notices to produce.

3.8 Section 280(1)(a) of the *Telecommunications Act 1997* provides for the disclosure of information if:

> … in a case where the disclosure or use is in connection with the operation of an enforcement agency – the disclosure or use is required or authorised under a warrant.

3.9 EFA state that:

> We believe that the Telecommunications Act overrides [the ability of agencies to submit compulsory notices to produce under their own legislation] and therefore, once the interception Bill is passed it will then override the Telecommunications Act and, as a result, civil penalty agencies and criminal penalty agencies will need to provide a warrant. There are not notice-to-produce provisions. [4]

3.10 However, during the Inquiry it was noted that there have been instances in the past where various government agencies have had differing views about the kinds of warrants they needed to access information from a carrier.[5]

3.11 Advice from ASIC indicates that, in their view, subsections 282(1) and (2) of the *Telecommunications Act 1997*, allows them to obtain stored communications using their notice to produce powers.[6]

3.12 The Attorney-General's Department supports the view that upon enactment of the proposed Bill, the position in relation to stored communications would be clarified and access to stored communications will only be permitted with a warrant.[7]

---

2 Explanatory Memorandum, p. 7-8.

3 Electronic Frontiers Australia, *Submission 3*, p. 24.

4 Ms Graham, *Committee Hansard*, 15 March 2006, p. 8.

5 Ms Graham, *Committee Hansard*, 15 March 2006, p. 8.

6 Australian Securities and Investments Commission, *Submission 13B*, p. 2.

Committee view

3.13 The Committee notes EFA's concern regarding the ability of a carrier to know whether or not the intended recipient has been notified of access to communications prior to the disclosure of such information. However, the Committee considers that there are means by which an enforcement agency can inform the carrier of notification to the intended recipient.

3.14 The Committee considers that distinction between overt and covert access to communications as provided for in the Bill, is a critical one. The Committee considers that covert access to communications must be subject to much tighter controls than overt access. Where access is covert, individuals have virtually no opportunity to protect privileged information or to challenge the grounds on which such access was granted.

3.15 Given that many law enforcement agencies will be unable to access a stored communications warrant for covert access to stored communications, the Committee recognises the need of enforcement agencies to have an overt means of access. This requirement is satisfied through the ability of agencies to use notices to produce where the intended recipient has been notified.

3.16 The Committee acknowledges the view that when enacted the current Bill will prohibit covert access to stored communications except where an agency has a stored communications warrant.

3.17 However, the Committee also acknowledges the importance of clarifying the regime governing access to stored communications particularly for the benefit of telecommunication carriers who carry the risk of criminal and/or civil action if they disclose stored communications information in breach of the *Telecommunication Act 1997* or the *Telecommunications (Interception) Act 1979*.

Recommendation 1

3.18 The Committee recommends that the Bill be amended to include a provision amending Section 280 and subsections 282(1) and (2) of the *Telecommunications Act 1997*, effective from the same date as the Bill, to make it clear that covert access to stored communications is not permitted without a stored communications warrant.

Stored communications warrants

3.19 Under the proposed amendments a stored communications warrant will be required to access stored communications held on the carrier's equipment. The inquiry identified a number of concerns regarding the proposed warrant regime for access to stored communication, in particular:

7 Mr McDonald, *Committee Hansard*, 15 March 2006, p. 41.

- offences for which stored communications can be accessed and used; and
- enforcement agencies for which access to stored communications may be granted.

Offences for which stored communications may be accessed and used

3.20 As noted above, the proposed amendments provide an exemption to the general prohibition for stored communications accessed with a stored communications warrant. The Bill proposes two penalty thresholds that must be met in relation to accessing and the use of, stored communications. The Bill provides an initial penalty threshold that must be met for a stored communications warrant to be issued. A lower penalty threshold is then specified for the secondary use and disclosure of information which has been accessed under a stored communications warrant.

The threshold for issuing a warrant

3.21 Proposed section 116(1)(d) provides that stored communications warrants may be issued to agencies if the information likely to be obtained would assist in connection with an investigation of 'serious contraventions'.

3.22 Serious contraventions are defined at proposed section 5E as:

> (1) a contravention of a law of the Commonwealth, a State or a Territory that:
>
> (a) is a serious offence;[8] or
>
> (b) is an offence punishable:
>
> (i) by imprisonment for a period, or a maximum period, of at least 3 years; or
>
> (ii) if the offence is committed by an individual – by a fine or a maximum fine, of at least 180 penalty units; or
>
> (iii) if the offence cannot be committed by an individual – by a fine, or maximum fine, of at least 900 penalty units; or
>
> (c) would, if proved, render the person committing the contravention liable to:
>
> (i) if the contravention is committed by an individual – a pecuniary penalty, or maximum pecuniary penalty, of at least 180 penalty units; or
>
> (ii) if the contravention cannot be committed by an individual – a pecuniary penalty, or maximum pecuniary penalty, of at least 900 penalty units.

3.23 The offences for which a stored communications warrant may be issued, are significantly less than those offences for which the existing telecommunications

8 As defined in the proposed amendment to section 5D – schedule 4, item 7 of the Bill.

warrants are currently available. That is, offences punishable by imprisonment for a period, or maximum period, of at least seven years.

3.24 The Attorney-General's department advised the Committee that the distinction between real time communications and stored communications, had been recommended by the Blunn report and is based on the supposition that something that is in writing, such as emails or a text message, is 'something that definitely involves more consideration of the expression'.[9]

3.25 However, other witnesses argued that the different treatment of the two forms of communications was unjustified:

> It strikes me as nonsensical that a differentiation would be drawn between speaking to somebody on a mobile phone and sending them an SMS message. Many of the students who I teach today see them as equivalent forms of communications. It makes no sense as a matter of law or public policy why, indeed, it is easier to gain one type of information than the other … I think the proper focus for assessing this legislation is: what is the appropriate limitation upon the privacy of Australian people? For them there is no rational distinction, so I cannot see how you could justify one from the government's end.[10]

3.26 This is supported by others who argue that the proposed penalty threshold for the issuing of a stored communications warrant is too low. The Australian Privacy Foundation states:

> The principle that invasion of privacy through covert interception should only be allowed in relation to genuinely serious offences is clearly established in the existing regime. In our view, no convincing case has been mounted for why a lower threshold should apply to stored communications, which can contain information just as private, sensitive and even intimate. In the absence of any such case, it is difficult to have a rational discussion about where the threshold should be set, but we strongly urge the Committee to recommend higher thresholds than those proposed.[11]

3.27 In contrast, law enforcement agencies such as the Australian Securities and Investment Commission (ASIC) and the Australian Consumer and Competition Commission (ACCC) state that the initial three-year threshold was too high and would severely impact on the ability to carry out their legislative function. The ACCC believes that their 'ability to obtain a stored communications warrant under the Bill appears … to be quite limited.'[12]

---

9 Mr McDonald, *Committee Hansard*, 15 March 2006, p. 39.

10 Prof. Williams, *Committee Hansard*, 15 March 2006, pp 28 and 31.

11 Australian Privacy Foundation, *Submission 4*, p. 5.

12 Australian Competition and Consumer Commission, *Submission 8*, p. 6.

3.28 ASIC argued:

> The specific issue we have with the draft bill in its current form is the threshold for obtaining the warrant – three years or 180 penalty units. We have many examples of provisions throughout the Corporations Act which address serious misconduct which have a lower threshold than that. … That means that we will not be able to access that material during the course of our investigation and that will affect, to a varying degree – depending on what the information is – our investigation and our ability to assess whether or not misconduct has occurred and then our ability to take action if it has occurred.[13]

The threshold for use

3.29 The proposal in the Bill to allow for information obtained under a stored communication to be used in proceedings into offences carrying a punishment of twelve months imprisonment or sixty penalty units was supported by enforcement agencies as an appropriate threshold.[14]

3.30 However, the lower secondary threshold was strongly opposed by other organisations. EFA state that they are:

> … opposed to the provisions allowing accessed information to be disclosed and used in relation to offences and contraventions involving the much lower penalties than those for which a stored communications warrant is permitted to be used.[15]

3.31 The Attorney-General's department explained that the stored communications regime has been designed to mirror the telecommunications regime in the sense that once the higher threshold has been met for the initial privacy intrusion, the penalty for the use of that information is then dropped.

Enforcement agencies for which access may be granted

3.32 The proposed section 110 provides that an 'enforcement agency may apply to an issuing authority for a stored communications warrant in respect of a person.' The Bill inserts a new definition of enforcement agency into subsection 5(1) of the Act. It defines an enforcement agency as having the same meaning as in section 282 of the *Telecommunications Act 1997* and also includes an interception agency and eligible authority of a State.

3.33 The Explanatory Memorandum further explains that enforcement agencies 'include all the law enforcement agencies responsible for investigating criminal matters, as well as agencies responsible for administering a law imposing a pecuniary

---

13 Ms Macaulay, *Committee Hansard*, 15 March 2006, pp 16-18.

14 Australian Securities and Investment Commission, *Submission 13,* p. 2.

15 Electronic Frontiers Australia, *Submission 3,* p. 18.

penalty or administration of a law relating to the protection of public revenue.'[16] Examples of enforcement agencies include the Australian Tax Office, the Australian Securities and Investment Commission and the Australian Customs Service.

3.34 It has been argued that the range of agencies that are able to apply for stored communications warrants should be limited. The Australian Privacy Foundation considers that the extension to the breadth of access provided for in the Bill 'strikes the wrong balance between protection of privacy – the acknowledged focus of the legislation, and the exceptions for other public interests.'[17]

Committee view

3.35 The Committee acknowledges the view of law enforcement agencies relating to their requirements to access stored communications in the course of investigations related to their legislative functions.

3.36 However, the Committee notes advice from ASIC that:

> The majority of our access to emails, however, comes from access at the user's end[18]

3.37 Further the Committee notes advice that 'in the last 12 months ASIC has not accessed stored communications from an ISP.'[19]

3.38 The Committee believes that this suggests that the need for enforcement agencies to seek access to stored communications via the carrier would be limited and a general prohibition of access to stored communications would only have limited impact, if any, on the work of these agencies.

3.39 The Committee agrees that an extension of agencies for which a stored communication warrant would be available 'strikes the wrong balance' between individual privacy and effective law enforcement. The key distinction is between covert and overt searches and the principal test should be the impact on individual privacy. The Bill would result in a wide number of government agencies being able to covertly obtain material for investigating a significant range of sometimes relatively minor offences.

3.40 The Committee is of the view that the invasion of privacy resulting from covert interception of communications is significant and should therefore only be accessible to core law enforcement agencies. As well, the Committee considers that offences for which stored communications warrants may be issued should be limited to criminal offences.

---

16 Explanatory Memorandum, p. 12.

17 Australian Privacy Foundation, *Submission 4*, p. 5.

18 Mr Inman, *Committee Hansard*, 15 March 2006, p. 17.

19 Australian Securities and Investments Commission, *Submission 13A*, p. 1.

3.41 Other agencies having a legitimate need to access stored communications may continue to use the notice to produce procedures under Section 280 of the *Telecommunications Act* (as discussed above), requiring the notification of the owner of the information.

Recommendation 2

3.42 The Committee recommends that the enforcement agencies able to access stored communications should be limited to those agencies eligible under the existing arrangements for telecommunications interception.

Recommendation 3

3.43 The Committee recommends that the Bill be amended to permit stored communications warrants to be issued only in relation to criminal offences.

Required warrant information

3.44 The Bill does not require that an application for a stored communications warrant, or the warrant itself, specify either identifying information for the subject of the warrant or any specific identifying information for the telecommunications services for which the warrant will authorise access.

3.45 EFA note in their submission that 'proposed section 6EB appears to assume that a stored communications warrant would contain information identifying the person and also identifying the relevant telecommunications service … However, it is not apparent from the Bill how the issuing authority would obtain such information.'[20]

3.46 The Attorney-General's department advised the Committee that:

> The warrant would include the name of the person whom the warrant is over, including the telecommunications services that the stored communications would be attached to. All the other relevant details would be included in the affidavit. The facts and the grounds for issuing or applying for the stored communications warrant are required to be included in the affidavit.[21]

3.47 Proposed section 118 of the Bill outlines the form and content of stored communications warrants. It provides that a stored communications warrant must be in accordance with the prescribed form and may specify conditions or restrictions relating to access. Notwithstanding the advice from the Attorney-General's department, the Committee notes that subsection 118(3) only requires that:

---

20 Electronic Frontiers Australia, *Submission 3*, p. 10.

21 Ms Hume, *Committee Hansard*, 15 March 2006, p. 37.

> A stored communications warrant must set out short particulars of each serious contravention in relation to which the issuing authority issuing the warrant was satisfied, on the application for the warrant …[22]

3.48 In addition, proposed sections 111-113, which deal with the application for a stored communications warrant and the accompanying affidavit information, do not require personal or telecommunications service identification information to be provided.

Committee view

3.49 To protect the integrity of the stored communications regime and the privacy of Australians, it is essential that both the subject of the warrant and the telecommunications services for which access is sought are clearly and unmistakeably identified in the application for a stored communications warrant and on the warrant itself. The Committee notes that existing section 42(4A) currently requires such identifying information to be included in the applications for named person warrants.

3.50 The Committee notes advice that:

> … the department is currently working on the prescribed forms for which the stored communications warrants will be made.[23]

3.51 The Committee considers that given the importance of clearly identifying the subject and services for which access is sought, the requirements for such information should be settled as soon as possible for inclusion in the Bill.

Recommendation 4

3.52 The Committee recommends that the Bill be amended to require applications for stored communications warrants, and the warrant itself, to include information that clearly identifies the person who will be the subject of the warrant and the telecommunications for which access is sought.

3.53 The Committee suggests that the existing provisions for named person warrants provide a suitable example of the type of information that ought to be required.

Safeguards and privacy protection

Issuing authorities

3.54 The proposed amendments extend the range of authorities who may be declared as issuing authorities for the purposes of the stored communications warrant regime. The proposed amendments allow for stored communication warrants to be

22 Proposed subsection 118(3)

23 Mr Gifford, *Committee Hansard*, 15 March 2006, p. 37.

issued by those identified as able to issue interception warrants, 'as well as any other Commonwealth, State or Territory judge or magistrate.[24]

3.55 It has been argued that allowing AAT members to issue telecommunication interception warrants has diminished the front end accountability of Australia's interception regime.[25] The NSW Council of Civil Liberties has suggested that the increase in the number of telecommunications interceptions is a result of allowing AAT members to issue interception warrants. The Council states:

> AAT members do not have tenure, are appointed by the government and work on contract. This means that AAT members are more likely to do the government's bidding than a judge, which explains why most warrants are issued by non-judges.[26]

3.56 Evidence was provided to the Committee which stated that the proposed extension of issuing authorities for the purpose of stored communications regime will make it too easy for enforcement agencies to obtain a warrant. The Australian Privacy Foundation argued:

> Restricting warrant issuing authority to judges, full time federal magistrates and full-time senior AAT members would be an important safeguard against it becoming too easy to for [sic] enforcement agencies to obtain a warrant.[27]

3.57 The Attorney-General's department explained the proposal to increase the range of issuing authorities as:

> … trying to get a balance. As ASIC said earlier, 'We don't see why these electronic things should be treated any different to any other hard copy document.' So you have that angle to it. Of course, a search warrant can be issued by a magistrate … I think Tony Blunn in his report makes this point that there is a distinction between something that is live and something that is being composed and stored like a document. Consequently, because of those factors, Mr Blunn recommended that it was appropriate to have it as a magistrate.[28]

Committee view

3.58 As discussed above, the Committee rejects the proposition that stored communications are equivalent to normal search warrants. The key differentiating factor is the covert nature of the stored communication warrant. For this reason, the

---

24 Explanatory Memorandum, p. 12.

25 Bronitt, S. and Stellios, J., Telecommunications interception in Australia: Recent trends and regulatory prospects, *Telecommunications Policy 29 (2005),* p. 886.

26 NSW Council of Civil Liberties, 'Australian phones 26 – times more likely to be bugged than an American phone', *Media Release,* 13 January 2006.

27 Australian Privacy Foundation, *Submission 4,* p. 4.

28 Mr McDonald, *Committee Hansard,* 15 March 2006, p. 39.

Committee does not accept that stored communications should be afforded any less privacy than is afforded to real time communications.

3.59 As such, the Committee does not consider a comparison between stored communications and hard copy documents justifies an extension of the issuing authorities to include magistrates. It is also noted that no evidence has been produced to suggest that the current arrangements are inadequate. In practice, an increase in the number of issuing authorities seems likely to make stored communications warrants more readily available.

Recommendation 5

3.60 The Committee recommends that the Bill be amended to allow issuing authorities to only include those currently able to issue interception warrants.

Enforceability in relation to State/Territory agencies

3.61 EFA highlight in their submission that while the Bill intends to regulate access to, and the use of, stored communications it is not clear if the Commonwealth would have the ability to enforce the provisions proposed in the Bill. According to EFA:

> In the case of interception information, this issue is dealt with by the legislated requirement that State and Territory Parliaments enact complementary interception legislation applicable to their agencies and responsible Minister prior to the (C'th) Minister being permitted to declare such agencies as 'eligible' interception agencies … However, there is no indication in either the Bill or Explanatory Memorandum of any intent to require State/Territory Parliaments to amend their interception legislation to complement the Commonwealth provisions concerning use, communication and recording of information obtained by accessing stored communications, and related reporting requirements.[29]

3.62 EFA advised the Committee that the issue would be remedied by requiring, as a precondition to being granted the powers of an enforcement agency under the stored communications regime, State and Territory Parliaments to enact complementary legislation. Given the tight timeframe for the implementation of such measures, as an additional safeguard EFA suggests that the Minister could be given the power to 'remove from state or territory agencies the right to get a warrant under the Commonwealth Telecommunications (Interception) Act.'[30]

3.63 This would provide similar protections as those provided by existing section 34 for telecommunications interception which allows the Minister, 'by legislative instrument and at the request of the Premier of a State, declare an eligible authority of that State to be an agency for the purposes of this Act' subject to certain conditions.

---

29 Electronic Frontiers Australia, *Submission* 3, pp 16-17.

30 Ms Graham, *Committee Hansard*, 15 March 2006, p. 14.

Committee view

3.64 The Committee considers it essential that the Commonwealth has the ability to enforce the obligations prescribed in the Bill relating to accessing stored communications. Immediate action should be taken to ensure enforceability of these provisions on State and Territory agencies.

3.65 The Committee considers that consistent with the arrangement for the existing telecommunications interception regime, State and Territory Parliaments should be required to enact complementary legislation for access to stored communications as a precondition to being granted the powers of an enforcement agency under the stored communications regime.

3.66 In light of the tight timeframe, the Committee supports the idea of amending the Bill to enable the exclusion of particular State/Territory agencies as an interim measure.

Recommendation 6

3.67 The Committee recommends that, consistent with the existing arrangements for telecommunications interception, immediate action be taken to ensure the enforceability of the stored communications provisions on State and Territory agencies by requiring complementary legislation to be enacted as a precondition to being granted the powers of an enforcement agency under the stored communications regime.

Recommendation 7

3.68 The Committee also recommends that as an interim measure, the definition of an enforcement agency in the Bill be amended to allow for the ability to exclude an agency specified in the Telecommunications Interception Regulations from being able to obtain a stored communications warrant.

Matters which issuing authorities must consider

3.69 The Bill proposes at section 116(2) that issuing authorities must have regard to:

(a) how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant; and

(b) the gravity of the conduct constituting the serious contravention; and

(c) how much the information referred to in paragraph (1)(d) would be likely to assist in connection with the investigation; and

(d) to what extent methods of investigating the serious contravention that do not involve the use of a stored communications warrant in relation to the person have been used by, or are available to, the agency; and

(e) how much the use of such methods would be likely to assist in connection with investigation by the agency of the serious contravention; and

(f) how much the use of such methods would be likely to prejudice the investigation by the agency of the serious contravention, whether because of delay or for any other reason.

3.70 The proposed approach is generally supported. However, it is suggested that that the issuing authority should be permitted to take additional considerations into account such as length of time stored communications have been stored and whether a search can be undertaken to obtain the relevant information.[31] Further, whether or not the stored communications are likely to include communications the subject of legal professional privilege and whether such communications should be placed in confidential safekeeping of an independent person should also be considered.[32]

Committee view

3.71 The Committee is of the view that individual privacy protection ought to be the chief consideration in any regime permitting access to personal communications. This is particularly important where communications may include information subject to legal professional privilege. The Committee considers that additional considerations for issuing authorities such as those suggested above will only serve to enhance the privacy protection already outlined in the Bill.

Recommendation 8

3.72 The Committee recommends that the Bill be amended to allow issuers of stored communications warrants to have regard to the length of time stored communications may have been held on a carrier's equipment and whether the communications sought can be sufficiently identified in order to minimise the impact on privacy.

Recommendation 9

3.73 The Committee also recommends that the Bill be amended to require issuers of stored communications warrants to consider whether the stored communications are likely to include communications the subject of legal professional privilege and whether any conditions may be implemented to prevent the disclosure of such communications.

Destruction of irrelevant information

3.74 Access to stored communications, by its very nature, results in the increased likelihood of the collection of large amounts of information that may not be relevant to the investigation for which the warrant was issued. Therefore, adequate provisions governing the destruction of irrelevant material are a vital privacy safeguard.

---

31 Electronic Frontiers Australia, *Submission* 3, pp 13-14.

32 Electronic Frontiers Australia, *Submission* 3, pp 13-14.

3.75 Proposed section 150 provides for the destruction of records obtained by accessing a stored communication. Specifically it states that:

> if the chief officer of the agency is satisfied that the information or record is not likely to be required for a purpose referred to in subsection 139(2); the chief officer must cause the information or record to be destroyed forthwith.[33]

3.76 In their submission, the Office of the Privacy Commissioner suggested that the effect of proposed section 150 may result in it being 'lawful for an agency to keep irrelevant information indefinitely.'[34] This is due to the fact that an obligation to destroy irrelevant information does not arise until after the chief officer has formed a view that the information is no longer required without the Bill specifying a time limit for this to occur.

3.77 The Office of the Privacy Commissioner recommended that, consistent with good privacy practice:

> consideration be given to amending the Bill to ensure that agencies take regular steps to review whether information they have accessed via stored communications warrants is still required for a permitted purpose eg; by setting a maximum period for review.[35]

3.78 The Attorney General's department argued it did not expect that any law enforcement agency that is permitted to access stored communications would fail to assess irrelevant information on a regular basis. As well, they advised the Committee that 'there is also the additional safeguard that there is a prohibition on the use of any information.'[36]

Committee view

3.79 The Committee considers that setting a maximum period for review of information obtained via a stored communications warrant will require agencies to establish procedures to deal with irrelevant information in a timely manner. Given the potential to collect vast amounts of irrelevant information under a stored communications warrant the Committee believes that such a safeguard is essential.

3.80 The Committee notes the assurances of the Attorney-General's department that the relevance of collected information would be considered in a timely manner, however these are not requirements that are contained in law. The legislation must also guard against any lapses in administrative practices within agencies. Furthermore, the Committee considers that such a requirement is particularly important given the

---

33 Proposed section 150(1)(b)

34 Office of the Privacy Commissioner, *Submission 6*, p. 2.

35 Office of the Privacy Commissioner, *Submission 6*, p. 2.

36 Mr Gifford, *Committee Hansard*, 15 March 2006, p. 42.

proposal in the Bill to extend the access to stored communications to a range of agencies that are not used to dealing with intercepted material as a matter of course.[37]

Recommendation 10

3.81 The Committee recommends that the Bill be amended to specify time limits within which an agency must both review their holdings of information accessed via a stored communications warrant and destroy information as required under the proposed section 150.

Monitoring of the stored communications warrant regime

Proposed reporting requirements

3.82 The Bill proposes lower reporting requirements for the use and effectiveness of stored communications warrants in comparison to the existing telecommunication interception warrants. The Explanatory Memorandum states that the reporting requirements for stored communications warrants are not as burdensome on the agencies as the reporting requirements for interception and these are consistent with general search warrant provisions and reflect the lower threshold to be met.[38]

3.83 However, the primary consideration of a regime which permits access to personal communications ought to be the protection of privacy. Stored communications warrants can not be considered the equivalent of search warrants due to their covert nature.

3.84 In their submission, EFA argues:

> Reporting obligations are necessary due to the covert and secretive nature of warrants and resultant potential for abuse. The fact that warrants will be available in relation to contraventions involving lesser penalties increases, not decreases, the potential for abuse.[39]

Role of the Ombudsman

3.85 The proposed amendments expand the functions of the Ombudsman considerably to include oversight of the stored communications regime. Section 152 proposes additional functions including:

> (a) to inspect an enforcement agency's records in order to ascertain, so far as is practicable, the extent of compliance, in relation to those records with sections 150 and 151; and
>
> (b) to report to the Minister about the results of inspections under this Division; and

37 Senator Payne, *Committee Hansard,* 15 March 2006, p. 42.

38 Explanatory Memorandum, p. 13.

39 Electronic Frontiers Australia, *Submission 3,* p. 19.

(c) to do anything incidental or conducive to the performance of any of the preceding functions.

3.86 In his submission the Ombudsman advised the Committee that:

> Whether my office is able to inspect most, if not all, agencies, in the spirit of the proposed amendments, or whether we will be able to inspect only a few, will depend on whether additional resources are available.[40]

3.87 The Ombudsman also advised the Committee that if a considerable number of enforcement agencies were inspected, the reporting timeframes may be difficult to meet. The Ombudsman went on to suggest:

> It would be preferred if the proposed reporting timeframes for section 153 reports could be extended to six months instead of three. This should not interfere unduly with the accountability objective while allowing more time for reports to be prepared that are as useful and comprehensive as they can be.[41]

Committee view

3.88 The Committee agrees with the view that reporting obligations are vital to provide adequate transparency and accountability for the stored communications warrant regime. The Committee agrees with the position that a lower offence threshold does not equate to a lesser reporting obligation.

3.89 As well, the Committee considers that the Ombudsman will undertake a vital role in the oversight and inspection of the stored communication regime. The Committee acknowledges the view expressed by the Ombudsman with regard to the impact that resources will have on his ability to fulfil the additional functions required under the Bill. The Committee is of the view that limited resources should not prevent adequate oversight of this regime. Therefore, the Committee considers that the Government should review the funding levels of the Commonwealth Ombudsman to provide the requisite additional resources to adequately fulfil this expanded function.

3.90 The Committee also supports allowing an additional three months to enable the production of useful and comprehensive reports.

Recommendation 11

3.91 The Committee recommends that Bill be amended to require agencies and the Minister to report on the use and effectiveness of stored communications warrants in a manner equivalent to the existing reporting obligations for telecommunications interception warrants.

---

40 Commonwealth Ombudsman, *Submission 10*, p. 2.

41 Commonwealth Ombudsman, *Submission 10*, p. 3.

Recommendation 12

3.92 The Committee recommends that additional resources be provided to the Ombudsman to enable the Office to fulfil the expanded functions under this Bill.

Recommendation 13

3.93 The Committee recommends that the Bill be amended to extend the timeframe for section 153 reports to six months.

Stored Communications and related definitions

3.94 The Bill inserts new definitions into the Act to support the establishment of the stored communications access regime.

3.95 Stored Communications is defined by the Bill as:

> … a communication that:
>
> (i) has passed over a telecommunications system; and
>
> (ii) is not passing over a telecommunications system; and
>
> (iii) is held on equipment that is operated by, and is in the possession of, a carrier; and
>
> (iv) is accessible to the intended recipient of the communication.

Copies of stored communications

3.96 In relation to the definition of stored communications as proposed in the Bill, EFA argues:

> In our view the definition results in insufficient clarity and certainty in relation to some types of records of communications held on carriers' equipment. For example, it is not clear whether a **copy** of a stored communication that is stored on a carriers' equipment, but is **not** accessible to the intended recipient of the communication, is to be regarded as a 'stored communication' or not.[42]

3.97 EFA suggest that copies of communications stored in a sender's sent box on a carrier's equipment, or communications stored on a carrier's backup device are examples of communications which may be regarded as copies of communications rather than stored communications.

3.98 The Attorney-General's department advised:

> A copy of a stored communication accessed by the person on the premises – so any end point of the communication – will not require a stored communications warrant. It is only those communications which are

42 Electronic Frontiers Australia, *Submission 3,* p. 6.

> accessed directly from the carrier which will require a stored communications warrant.[43]

Definition of accessing a stored communication

3.99 In their submission, EFA highlight that accessing a stored communication as provided for in section 6 of the Act refers to among other things, 'recording such a communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication.'[44]

3.100 However, recording a communication, as defined in the Act, does not specifically address recording in relation to accessing a stored communication.

3.101 EFA suggest that:

> The definition of a record should be amended so that it applies in relation to, not only an interception, but also accessing a stored communication.[45]

Access to stored communications via the sender

3.102 In regard to the definition of stored communications, Telstra advised that it appears to limit stored communication warrants to accessing communications **received** by a person of interest, but not those communications **sent** by the person of interest. Telstra stated that:

> Carriers cannot necessarily know whether, or when, a communication that has been sent has been received by the intended recipient and, therefore, whether a communication that has been sent has become a stored communication. As such, communications that have been received by a person of interest would be stored communications, and could be accessed under a stored communications warrant. In contrast, communications that have been sent by the person of interest would not be stored communications, and therefore, could not be accessed under a stored communications warrant.[46]

3.103 The Attorney-General's department advised the Committee that:

> That question, of whether or not access is available via the sender, is still under active consideration by the government in terms of making sure it makes sufficient allowance for our operational needs.[47]

---

43 Mr Gifford, *Committee Hansard,* 15 March 2006, p. 36.

44 Proposed section 6AA

45 Electronic Frontiers Australia, *Submission 3,* p. 8.

46 Telstra, *Submission 20,* p. 2

47 Mr Gifford, *Committee Hansard,* 15 March 2006.

Unsolicited commercial electronic messages

3.104 In their submission, the Australian Communications and Media Authority (ACMA) highlight that as currently drafted the definition of stored communications would adversely impact the ACMA's ability to enforce the *Spam Act 2003* (the Spam Act). ACMA state that:

> … any spam message that falls outside the definition of a stored communication will not be accessible by ACMA investigators under the proposed warrant regime and would therefore be unavailable to ACMA investigators in their enforcement of the Spam Act.[48]

3.105 The Attorney-General's department advised the Committee that:

> This is an issue that ACMA has raised with us previously. It is a matter on which we continue to work collaboratively with ACMA and the Attorney is well versed on this particular issue.[49]

3.106 The Committee is of the view that it is essential that the definitions proposed in the Bill provide sufficient clarity to support the effective operation of the stored communications warrant regime. The Committee acknowledges the advice from the Attorney-General's department that in some cases work is continuing. However, the Committee considers that definitional issues should be settled prior to the passage of the Bill.

Recommendation 14

3.107 The Committee recommends that the Bill be amended to ensure that copies of communications can not be accessed without a stored communications warrant.

Recommendation 15

3.108 The Committee recommends that the definition of 'record' be amended so that it applies in relation to accessing a stored communication.

Recommendation 16

3.109 The Committee recommends that the issue regarding whether or not access to stored communications is accessible via the sender is settled and the Bill be amended as necessary.

Recommendation 17

3.110 The Committee recommends that prior to the passage of the Bill the definition of stored communications be amended so that the Australian

48 Australian Communications and Media Authority, *Submission 18*, p. 2.

49 Mr Gifford, *Committee Hansard*, 15 March 2006, p. 34.

Communications and Media Authority's ability to enforce the Spam Act is not limited.

Peer-to-peer networks

3.111 The proposed definition of stored communication provides that a stored communication is defined to mean a communication that, among other things, is held on equipment operated by the carrier at its premises. The Explanatory Memorandum states that:

> This is to ensure that … the stored communications regime only applies to accessing stored communications via a telecommunications carrier. The regime does not affect existing lawful access to communications stored on a person's telecommunication device.

3.112 Communications are not considered 'stored communications' if they are unable to be accessed via the carrier. However, current technology allows individuals to share content files[50] via the peer-to-peer model (file sharing). The peer-to-peer model allows files to be stored on and served by personal computers of the users. Pure peer-to-peer networks do not have a central server managing the network or a central router.

3.113 Since the stored communications regime applies only to communications held by a telecommunications carrier, it will not extend to allow access to other communications and information shared via a peer-to-peer network. This may therefore, allow persons of interest to avoid covert access to their stored communications by law enforcement agencies.

3.114 The intent of the Bill has been described as assisting 'law enforcement and security agencies to keep pace with increasingly sophisticated methods of avoiding detection.'[51] The Committee acknowledges the challenges associated with developing technology neutral interception and access regimes, particularly given rapid technological advances. However, increased use of peer-to-peer technology is likely to have a considerable impact on the effectiveness of the stored communications regime proposed in the Bill.

---

50 Content files can contain audio, video, data or anything in digital formal, as well as real-time data, such as Voice over Internet Protocol.

51 Ruddock, P., *Interception amendments achieve appropriate balance*, Media Release, 16 February 2006.