CHAPTER 4

DEVICE-BASED NAMED PERSON WARRANTS

4.1 A broad range of witnesses raised concerns in relation to the proposal in the Bill to permit devices to be added to a warrant after it had been issued and without further reference to the issuing authority, and for the identification of devices in warrants only to the extent that it is known. These witnesses, which included the Law Council of Australia (the Law Council), the Castan Centre for Human Rights Law (Castan Centre), Privacy Commissioners and civil liberties groups, (collectively privacy and civil liberties groups), considered that the proposed amendments represented an extension of interception powers that would result in innocent persons who were not the subject of investigation having their privacy invaded. These concerns are discussed in greater detail below, under the following broad subject headings:

- Tension between privacy rights and the need for interception powers;
- Identification of devices;
- Adding devices to device-based warrants after issue;
- Accountability mechanisms;
- Consistency between service-based and device-based warrants;
- Legislative intent concerning device-based named person warrants; and
- Suggestions for safeguards if devices are added to warrants.

4.2 The chapter incorporates committee conclusions in each section where appropriate.

The tension between privacy and the need for interception powers

4.3 Evidence heard by the committee was primarily divided between two viewpoints. Submissions by police forces[1] and the Attorney General's Department (the Department) considered the amendments were needed by interception authorities for operational purposes. Conversely, privacy and civil liberties groups considered the amendments unsatisfactory in relation to the protection of individuals' rights to privacy and public accountability standards.

4.4 The committee received evidence that the impact from a privacy perspective was significant and potentially inconsistent with community expectations. For example, the Victorian Privacy Commissioner submitted that:

> The effect of this bill on the privacy of individuals is significant.

---

1 *Submission* 9, pp 1-3; *Submission* 12, pp 1-3; *Submission* 13, pp 1-2; *Submission* 14, p. 1.

> With the increase in uptake and use of technology, communication over the internet and telephones (including mobile phones) is the primary method of communication today. Individuals communicating through telecommunications devices are likely to exchange all sorts of information, ranging from private health information to personal business affairs, the nature of professional advice received as well as sensitive information concerning their health, sexual orientation and practices, political opinions and religious views.
>
> Australians have the right to expect that the State will not intercept or access their communications without just cause and due process. The greater impact a warrant will have on an individual's rights (including their right to privacy), the more stringent the requirements for obtaining the warrant should be. If granted, any warrant should be as specific, finite and limited as is reasonable in achieving its aims. In particular, the ability of the warrant system to protect individual privacy depends on the issuing authority considering each individual device from which telecommunication are to be intercepted under the warrant.[2]

4.5 Conversely, while acknowledging privacy issues, the Victoria Police's submission expressed its need for these amendments from a law enforcement viewpoint:

> There is clearly an operational need for Law Enforcement Agencies to be able to obtain a single warrant which authorises the interception of multiple devices used or likely to be used by the suspect and which allows additional devices to be added to a warrant if and when they are identified. …
>
> Service-based named person warrants exist to allow multiple services to be intercepted in connection with one named person warrant and also additional services to be added to a warrant if and when they are identified. The proposed amendment will allow the provisions governing the issue of device-based named person warrants to be brought into line with the provisions governing the issue of service-based warrants.
>
> The expanding use of telecommunication interception powers as an investigative tool and the associated concerns that this may give rise to, such as issues of privacy and the expansion of police powers, are always relevant factors. However, the amendment merely provides a means of obtaining evidence in a more timely manner than is currently possible under existing legislation.[3]

4.6 Representatives of the Department explained that interception agencies need the operational flexibility to adapt to changing technology, noting that while the legislation is intentionally technologically neutral, changes in technology have required legislative amendment to maintain operational effectiveness:

---

2 *Submission* 5, p. 2.

3 *Submission* 9, p. 2.

> Advances in technology have created a market where multiple communications are the norm due to the low cost associated with purchasing telecommunications services. This is creating an environment whereby it is reasonably inexpensive to purchase multiple communications devices such as mobile phone handsets or laptop computers. These devices, when combined with the availability of multiple services, provide opportunities for evading detection by law enforcement agencies…
>
> …
>
> To meet community expectations that serious criminal offences are investigated and prosecuted, it is important that law enforcement [and] national security agencies can quickly adjust to this changing environment.[4]

4.7 The committee acknowledges the tension between the need for interception agencies to have the necessary powers to safeguard the community; and the requirement to protect individuals' rights to privacy, particularly those persons who are not associated with a particular investigation. These objectives need to be balanced in any legislative amendment that involves new powers, or an extension of powers.

Identification of devices

4.8 The accurate identification of telecommunications devices to be intercepted is contentious because of the potential to intrude upon the privacy of innocent people if devices are not correctly identified before interception commences. The submission made by the Law Council illustrated two examples of how an unjustified invasion of a person's privacy might inadvertently occur:

> ASIO or a law enforcement agency may have correctly identified their suspect *but* may have erroneously identified the telecommunications services or devices used by that person, (again perhaps on the basis of incomplete or unreliable information), with the result that the communications of an innocent third party are intercepted.
>
> ASIO or a law enforcement agency may have correctly identified their suspect and correctly identified the telecommunication service or devices used by that person *but* may not be technically able to uniquely identify telecommunications made using that service or device without the risk of intercepting communications made via an unrelated service or device (This appears to be more of a real risk with device-based, rather than service-based interception…).[5]

4.9 The Law Council concluded that 'the proposed amendments will significantly reduce the role of the warrant authorisation process in safeguarding against errors of the kind…' illustrated above.[6]

---

4 *Committee Hansard*, 17 April 2008, p. 28.

5 *Submission* 1, p. 4.

6 *Submission* 1, p. 8.

4.10 In relation to identification of devices, several submissions[7] drew the committee's attention to previous examination of this issue in the Blunn report;[8] the committee's previous findings and recommendations in relation to the introduction of device-based warrants in the 2006 amendment bill; and/or the subsequent government response. These submissions questioned whether there had been further development to improve the reliability and accuracy of unique identifiers that the Australian Government had committed to progress, or whether this commitment was now being put aside.

4.11 For example, the Law Council submitted that:

> There is no information included in the material supporting the Bill to suggest that the concerns expressed by the Senate committee in 2006 about the accuracy and reliability of device based interception have been addressed. Nonetheless, the proposed amendments explicitly invite Parliament to treat device-based interception as no more risky or problematic than service based interception.[9]

4.12 The Department stated that unique identifiers are available for devices such as mobile handsets and laptops:

> All telecommunications devices, such as a mobile handset or a laptop computer, have a unique identifier that allows the device to interact with telecommunications. For example, the unique identifier for a mobile handset is called an International Mobile Equipment Identifier (IMEI). A unique identifier for a computer or any wireless connected device is a Media Access Control (MAC) address. It is possible to match the unique identifier of the device to a particular person via subscriber detail or through the monitoring of known telecommunications services that the person of interest is using.[10]

4.13 However, the committee also received evidence from the Department which suggested that accurately identifying a unique and indelible identifier of the source of telecommunications, as recommended in the Blunn report, remains an operational challenge. The Department provided the following scenario:

> There will be intelligence to say someone has walked into a particular shop and bought half a dozen phones plus 100 SIM cards, which is not an unusual scenario. The reality is, that until they use the phone, you cannot identify the unique identifier.[11]

---

7 Submission 1, p. 4; *Submission* 7, pp. 6-7; *Submission* 10, p. 2.

8 A.S. Blunn AO, *Report of the Review of the Regulation of Access to Communications*, 2005.

9 *Submission* 1, pp 5 and 7.

10 *Submission* 4, p. 3.

11 *Committee Hansard*, 17 April 2008, p. 33.

4.14 Further, there appears to be some doubt about the reliability of the unique device identifiers, due to the possibility that these may be altered. At the public hearing, a representative of Electronic Frontiers Australia (EFA) advised that altering the identification of a device was possible:

> In many if not most cases, those [device-based] identifiers can be altered, cloned or copied, so that they do not reliably provide a unique identifier. Moreover, we are given to understand that where suspects in criminal investigations, for example, might be seeking to avoid surveillance by law enforcement agencies, they might be minded to change identifiers to hide their tracks. In the types of situations in which these warrants might address this, there is perhaps a higher than normal chance that identifiers might not be unique.[12]

4.15 The Department acknowledged this concern, stating that:

> In a policy sense, we are working with the industry, ACMA [Australian Communications and Media Authority] and the Department of BCDE [Broadband, Communications and the Digital Economy] to look at ways to deal with this problem. There are offences in the Criminal Code for altering IMEIs [International Mobile Equipment Identifiers] and IMSIs [International Mobile Service Identifiers]—being the service number or the actual phone handset number—and the AFP [Australian Federal Police] enforces those particular laws in relation to changing IMEIs and IMSIs. But, of course, technology is very fast moving and people will always find ways to change numbers.[13]

4.16 The New South Wales Council for Civil Liberties (NSWCCC) submitted that allowing more devices to be intercepted without improving device identification accuracy was not acceptable on privacy grounds:

> A significant number of additional people will have their conversations and other messages listened to or read if this Bill is passed. These will include users of intercepted devices other than the targeted person, and those with whom they communicate. Until such time as devices are identifiable by unique identifiers and accidental interception of the wrong devices is eliminated, they will also include persons not connected in any way with the targeted person. The broader the range of devices which are targeted, the greater the increase in invasion of privacy.[14]

Adding devices to device-based warrants after issue

4.17 A major change proposed in the Bill relates to allowing interception agencies to add additional devices to a device-based warrant without further referral to an issuing authority. Many of the submissions and much of the evidence received at the

---

12 *Committee Hansard*, 17 April 2008, p. 18.

13 *Committee Hansard*, 17 April 2008, p. 34.

14 *Submission* 2, pp 2-3.

hearing objected to this proposed change, viewing it as a major extension of the existing provisions.

4.18 The following section of this report is laid out as follows:

- Paragraphs 4.19 – 4.22 set out a description, as primarily incorporated in the Attorney-General's Department's submission, of how privacy issues will be addressed and how accountability mechanisms will operate;
- Paragraphs 4.23 – 4.26 describe operational practices and needs, as put forward in evidence by police forces.
- Paragraphs 4.27 – 4.30 then return to the objections raised by privacy and civil liberties groups.

Requirements, process and safeguards

4.19 The Department described the existing two-tier process to address privacy in the issuing process for a device-based named person warrant. The first step is to establish that a device-based named person warrant is the only practical mechanism available to intercept telecommunications:

> The primary issue of the interference with a person's privacy is addressed by the issuing authority in considering whether to grant a device-based named person warrant. The interception agency must satisfy the issuing authority that:
>
> - there are no other practicable methods available at that time to identify the telecommunications services being used, or likely to be used, by the person of interest, or
> - it is impracticable to intercept the service being used by the person of interest.[15]

4.20 If the issuing authority is satisfied that a device-based named person warrant is appropriate to the circumstances, the issuing authority then must have regard to the following privacy considerations and other factors:

> - the impact the interception will have on the existing privacy of any persons as a result of intercepting communications made from any service or of a particular device used or likely to be used by the person of interest;
> - the extent to which alternative methods of investigation have been used by the interception agency; and
> - that the interception is for an investigation of a serious offence, generally punishable by a maximum period of imprisonment of at least seven years.[16]

---

15 *Submission* 4, p. 3.

16 *Submission* 4, p. 3.

4.21 The Department's submission also explained the internal procedures to which an interception agency would be required to adhere if the agency was permitted to add additional devices to a warrant without independent external scrutiny:

> The Bill allows the head of an agency or a senior officer or staff member of an agency who has been approved in writing by the chief officer of an agency, to approve the addition to the warrant of an additional device, and to notify the relevant carrier. The senior officer is not able to make decisions that go beyond the limits of the original warrant and therefore is required to be satisfied that the addition of a device to a named person warrant would meet the thresholds that an issuing authority must have regard to, or be satisfied of, in issuing the original warrant.[17]

4.22 The submission went on to explain the existing accountability mechanisms under the TIA Act that would be safeguards which might address issues raised by privacy and civil liberties groups:

- An interception agency is required to revoke a warrant when the grounds for the warrant no longer exist. This includes where it is no longer impracticable to intercept telecommunications being used by the person.
- Intercepted material must be destroyed where it is not relevant to the permitted purposes of the agency – generally an investigation of an offence that is punishable by three years imprisonment or more.
- An issuing authority may impose conditions or restrictions on an interception warrant.
- The Ombudsman has independent oversight of the conduct of the interception agencies in carrying out interception.[18]

Operational need for devices to be added after issue of the warrant

4.23 The committee received evidence from Victoria Police, the AFP and the Attorney-General's Department that operational effectiveness requires the timely interception of devices since:

> The evolving practice by the criminal element of utilising multiple SIM cards in multiple handsets has become a significant inhibitor to the detection of crime and the apprehension of offenders. LEA's [law enforcement agencies] once again will be at a disadvantage when trying to identify and subsequently intercept telecommunications in a timely manner. The 'educated' criminal element is already utilising such practices to defeat current methods of telecommunications interception and will continue to do so. The use of such tactics will certainly increase as it becomes more commonly known.[19]

---

17 *Submission* 4, p. 4.

18 *Submission* 4, p. 4.

19 *Submission* 9, p. 2.

4.24 Tasmania Police also noted that the amendments would 'provide for a greater effectiveness of the Telecommunications Interception warrant regime'.[20]

4.25 A representative of the AFP described the warrant process and need for timeliness to the committee from an operational perspective:

> …when you are seeking the grounds for the original warrant, you are at the earlier stage of the investigation. You do not have interception in place, so you are going through that accountability process. I do not think that anything we are saying or the department is saying is meant to undermine the importance of that up-front authorisation by an external body. What we are talking about is the fact that, in the overall architecture of the T(I) Act [TIA Act], a device based warrant is in the first place really the warrant of last resort. We have to be satisfied, and we need to be able to satisfy our internal processes and then the issuing authority, that a service based warrant or some other TI [telecommunications interception] warrant is not a better way to get access to the information that we are after to assist with our investigation. As that investigation progresses and we are aware or become aware that that person suspects that they are under surveillance by the police, that the police are interested in them, and they start undertaking those counter surveillance type activities, we need to be able to try and counter that to maintain our capability. That is why we are suggesting that, when it comes to adding a device to an existing warrant where we were not aware of the existence of that device when we first sought the warrant, an internal authorisation approach, on balance with the other accountabilities that are available in the Act, is the best way ahead from an operational perspective.[21]

4.26 A representative of the Department also described some of the internal accountability and approval requirements that will apply when a device is to be added subsequent to the issue of a warrant:

> …the decision to add another device will be made by a senior officer within the agency, which does sit separately from any of the actual investigation itself, so the objectivity does come in there. I should also say that they will not be able to add a device that is inconsistent with the purposes of the warrant in the first instance. There has to be not only the likelihood that the person is using it but the likelihood that the use of it is in relation to the offence for which the warrant was issued.…
>
> I should also say that, as a matter of best practice, the Attorney-General's Department must receive copies of all warrants.[22]

---

20 *Submission* 13, p. 2.

21 *Committee Hansard*, 17 April 2008, p. 33.

22 *Committee Hansard,* 17 April 2008, p. 31.

Scrutiny of devices added to a warrant

4.27 The committee heard evidence arguing that the provisions of the Bill that will permit interception agencies to add new devices to a warrant without further independent scrutiny by the issuing authority would adversely affect the privacy rights of individuals.

4.28 The Law Council firstly agreed with the statement in the Department's submission that 'the primary issue of the interference with a person's privacy is addressed by the issuing authority in considering whether to grant a named person warrant.'[23] However, the Law Council went on to state that:

> …it is difficult to see how the threshold test for privacy can be met where the issuing authority remains unaware of the particular devices to be targeted under the warrant.[24]

4.29 The Castan Centre elaborated on the privacy consequences of removing the requirement that an issuing authority scrutinise information pertaining to all devices in a warrant:

> At the time of issuing, the issuing authority does not know what those devices are or might be and so has no basis on which to adequately address the question of whether or not the interception of those further devices would interfere with the privacy of any person or persons in an inappropriate fashion. The concern arises particularly in relation to device based warrants because when one looks, for example, at the explanatory memorandum for the 2006 bill, which introduced the device based warrants, it makes it clear that the logic of a device based warrant is that it is useful when a device is being used in respect of multiple services. Of course the device might also be used by multiple users.
>
> So… it seems quite possible that some person, not of interest to the authorities and who was not identified in the warrant, might nevertheless be using the device to make a communication on some service or other and then become subject to interception pursuant to the warrant.[25]

4.30 The committee questioned several witnesses about whether the requirement to seek prior approval from an issuing authority before adding devices to a warrant imposed an additional 'red tape' burden on an interception agency, in terms of time and identifying the device. Witnesses were consistent in considering that prior approval is appropriate and necessary. Comments included:

- the 'red tape' includes existing safeguards and there is a significant difference between extra red tape and the removal of safeguards;[26]

---

23 *Submission* 1, p. 10.

24 *Submission* 1, p. 10.

25 *Committee Hansard*, 17 April 2008, p. 3.

26 *Committee Hansard*, 17 April 2008, p. 24.

- the requirement to seek approval is consistent with Australia's international human rights obligations;[27]
- there is a balance to be struck between the lawful interception needs of an agency and the needs of the public to be protected from the excesses and abuses to which those powers could conceivably be put. The purpose of device-based warrants is to address the issue of 'proliferation of SIM cards', that is, the ability to intercept multiple SIM cards in one device;[28]
- the proposed amendment is fundamentally inconsistent with the nature of the independent review. An analogy for this proposal is that of a magistrate issuing a search warrant that allowed the police not only to search a residence of a particular suspect but any other place in which it is 'likely' a person might be. It removes the need for showing proof and justification before an independent party;[29]
- the one additional step of obtaining a warrant should not be omitted, as the AFP states in its submission that interception agencies are required in any case to do the work to identify the additional devices;[30]
- none of the current safeguards prevent interception agencies doing their jobs;[31] and
- the community would expect that a documented case needs to be made to someone to justify the addition of a device, and that case should preferably be made to someone external, rather than internal to the agency actioning the warrant.[32]

Conclusions

4.31 The committee acknowledges that interception effectiveness needs to keep pace with technological changes and changes in the behaviour of criminals seeking to avoid detection. This may require ongoing legislative change unless more 'technologically neutral' legislation can be introduced.

4.32 The committee accepts that even a short delay may result in loss of valuable information and affect investigatory outcomes. This is clearly not ideal and, in certain circumstances such as life-threatening situations, may be unacceptable. However, any changes to existing powers and safeguards must always be weighed against the potential for additional intrusion into individual rights and privacy.

---

27 *Committee Hansard*, 17 April 2008, p. 8.

28 *Committee Hansard*, 17 April 2008, p. 20.

29 *Committee Hansard*, 17 April 2008, p. 20.

30 *Committee Hansard*, 17 April 2008, p. 8.

31 *Committee Hansard*, 17 April 2008, p. 24.

32 *Committee Hansard*, 17 April 2008, p. 12.

4.33 The committee accepts that the ability of interception agencies to rapidly respond to 'turnover' in the telecommunication devices being used by people being intercepted is somewhat constrained by the current device-based warrant regime. This problem would be reduced if interception agencies were able to apply for multiple devices in a single application for a warrant. Allowing agencies to add devices to a warrant subsequent to its issue may also increase the capacity of interception agencies to respond in an efficient and timely manner. However, the TIA Act does not currently permit either process.

4.34 The committee is of the view that as a general principle, it is unobjectionable for interception agencies to intercept multiple devices on a device-based named person warrant. The committee is not convinced, however that an issuing authority can adequately consider potential interference with the privacy of any person(s), and also consider the other factors against which this should be balanced, if it is unaware of the identity of the devices that an interception agency may add subsequently to a device-based named person warrant.

4.35 During the course of the inquiry, Departmental representatives argued that replacing external scrutiny of devices that an interception agency wishes to add to a device-based named person warrant with internal-to-department scrutiny would still achieve equivalent consideration of privacy issues. The Department explained that the officer who will assess applications for additional devices would not be from within the area where the application originates. Additionally, the Department asserted that the purpose of the interception of the additional device must be consistent with that in the original warrant, and that each device is subject to the same test of 'likelihood' that the person named in the warrant is using the device.

4.36 However the committee considers that these safeguards cannot fully substitute for independent scrutiny by an issuing authority. The amendments, if passed, would remove an important existing safeguard, that is, independent scrutiny of any devices that an interception agency wishes to intercept.

4.37 Privacy Commissioners, civil liberties and rights groups and the Law Council were unanimous in considering that independent scrutiny is not merely 'red tape'. In their view, removing an existing safeguard is different from objecting to new safeguards. The committee agrees with this view and, in particular, considers that:

- compared with service-based interception, device-based interception is more likely to result in the invasion of privacy of people not identified in the warrant;
- a balance should be maintained between the protection of the community by security and law enforcement agencies; and the accidental or deliberate infringements on privacy that can result from interception; and
- independent review should be an integral part of the balancing effect of these interception powers on other public rights.

4.38 However, the committee considers that intercepting agencies should only be permitted to add further devices to a device-based named person warrant after the warrant has been issued in defined circumstances, not as a general practice. Any devices added should be notified to the issuing authority within a limited period. The issuing authority should also have the power to declare that the interception should cease and all information gathered destroyed if the issuing authority decides that the facts of the case would not have justified the addition of the devices.

Accountability mechanisms

4.39 The Law Council disagreed with the Department's statement that existing accountability mechanisms are sufficient safeguards for these proposed amendments. The Law Council did not find these mechanisms satisfactory, commenting specifically that:

> All but one of these accountability mechanisms are directed at monitoring the use of interception powers after a warrant has been issued and executed.
>
> The Law Council submits that 'after the fact' reporting or oversight mechanisms are not an adequate substitute for a rigorous, external warrant regime which determines whether, when and how ASIO or police should be exercising interception powers in the first place.[33]

4.40 A representative of the Privacy Foundation, after being questioned by the committee on whether the privacy protections outlined by the Department were sufficient, said:

> There are two types of privacy safeguards: those inherent in the authorisation process and the downstream safeguards. It is true that the downstream safeguards in terms of reporting and the necessity to comply with certain record-keeping requirements will still apply, but the upstream safeguards, the ones that are delivered by the authorisation process, are in a sense negated by a multiple device based warrant because the issuing authority is simply not in a position to make the appropriate judgement about the balance of interests since they will not have any information, as we understand it, about which other individuals may be users of those devices. Therefore, the arguments about the likelihood of the suspect or the target using those is information that simply will not be made available to an issuing authority so that they can make the appropriate judgement about the balance of interests.[34]

4.41 The Castan Centre discussed the effect of removing independent scrutiny and broadening the range of telecommunications devices from which communications may be intercepted. They said that the effect would be to dilute the statutory obligations of interception agencies to justify interceptions. The Castan Centre commented that:

---

33 *Submission* 1, p. 11.

34 *Committee Hansard*, 17 April 2008, p. 23.

> One potential consequence of such a dilution of accountability would be to encourage the undertaking of 'fishing expeditions', as agencies become freer to form their own, untested, views as to which devices a person is likely to use. This also further exposes the communications of third parties, not named in the warrant, to the possibility of interception, which is objectionable…[35]

4.42 A representative of the AFP disagreed with this view, commenting that internal safeguards and accountability mechanisms are sufficient:

> We believe that, for the addition of a device to an existing warrant, the internal accountability would be the way to go, and those additional oversight mechanisms would be through the reporting arrangements and the oversight of the Ombudsman and its scrutiny of our processes, which is fairly regular. It is annual and regular.[36]

4.43 The Castan Centre's submission identified several areas where dilution of accountability has resulted in cases which 'strongly suggest that investigatory agencies need to be held more accountable in the exercise of their statutory powers, not less so.'[37] The submission emphasised that this was not just about protecting human rights, but also about preserving agencies' integrity, and requiring them to account for the exercise of their powers.

4.44 The Castan Centre provided two examples to support its argument:

- the recent arrest and subsequent release of Dr Mohammed Haneef; and
- the case of Izhar Ul-Haque, in which the judgement of Justice Adams of the New South Wales Supreme Court criticised the conduct of both ASIO and AFP officers.

4.45 The representative of the Privacy Foundation provided other examples of internal scrutiny and accountability failure, citing the leakage of information and its misuse by officers of the Australian Taxation Office and Centrelink. He also drew attention to what he described as the 'fairly regular' instances of police corruption and misuse of official information, mainly in state police forces.[38]

4.46 The representative of the Privacy Foundation argued that these types of occurrences did not give the confidence 'to simply sweep away the safeguards in the name of efficiency.' He went on to differentiate between the abuse of information and the 'more general, chilling effect of surveillance' as follows:

> We think one of the dangerous trends is the tendency of governments to assure us that extension of powers to monitor and surveil the activities of

---

35 *Committee Hansard*, 17 April 2008, p. 5.

36 *Committee Hansard*, 17 April 2008, p. 33.

37 *Submission* 8, p. 6.

38 *Submission* 10, p. 24.

> citizens is okay because, as they say, they will put in place the safeguards that deal with the abuse and suchlike. That, to our view, negates the important social value of privacy and freedom from surveillance as something that we actually treasure and, in most liberal democracies, value quite highly. It simply is not good enough to say, 'If you've got nothing to hide you've got nothing to fear.' We all have the right, in our view, to basically go about our business in private unless it needs to be intruded on. The threshold tests for that intrusion need to be kept as high as possible.[39]

Conclusions

4.47 The committee is of the view that 'after the fact reporting' is insufficient to adequately address issues associated with individuals' privacy and rights.

4.48 In regards to the accountability mechanisms internal to interception agencies, the committee commends the work done by interception agencies to improve their processes and accountability mechanisms. However, the internal processes of any agency, public or private, are susceptible to failure, whether this be accidental, by oversight or omission, or deliberate. The care and attention to preserving a (possibly unknown) individual's right to privacy can be lost in the pressure of work and the need to achieve results.

4.49 The committee considers that best practice is to maintain independent scrutiny, should agencies be authorised to add devices to a warrant, except in exceptional circumstances.

Consistency between service- and device-based warrants

4.50 The EM for the Bill states that the changes to the device-based warrant provisions establish a consistency with the service-based warrant provisions.[40] The committee concurs that the proposed amendments will, if passed, establish a consistency or equivalency in terms of wording.

4.51 While the police forces and the Department did not specifically identify why this consistency is desirable, they drew attention to the operational needs of interception agencies (as outlined above) and, by inference, the need for the device-based and service-based provisions to be consistent. The Department and the AFP confirmed that the current requirement for an issuing authority to scrutinise every telecommunications device added to a device-based named person warrant would be removed by the Bill. However, they argued that the current safeguards and accountability mechanisms contained in the TIA Act, together with internal guidelines and procedures within agencies, would be sufficient to ensure privacy and accountability issues are adequately addressed.

---

39 *Submission* 10, p. 24.

40 EM, p. 4.

4.52 The committee heard evidence from privacy and civil liberties groups and the Law Council that device- and service-based interception warrants are not similar in nature and that relaxing provisions for devices to achieve 'consistency' with services is undesirable. In particular, these groups considered that device-based warrants were more likely to lead to the invasion of privacy and civil rights than service-based warrants. These groups concluded that independent scrutiny of devices added to a warrant is necessary, at the very least.

4.53 The committee acknowledges that accurate identification of devices remains more difficult than for services, and inaccurate identification may lead to the interception of the communications of people who not relevant to the investigation. Compared with services, devices are also more susceptible to having their identification tampered with or 'stolen', and devices are easier to dispose of and replace, as outlined above.

4.54 The Castan Centre submitted that another difference between services and devices is the multi-user nature of devices compared with services, which will potentially lead to more non-suspects being intercepted on a particular device than a particular service. The Castan Centre concluded that amending device-based warrant provisions to make them consistent with service-based interceptions would increase interception powers, as follows:

> One significant consequence of this broadening of the range of telecommunications devices from which communications may be intercepted would be to permit further incidental monitoring of people who are themselves of no relevance to a particular investigation, but who happen to use a telecommunications device that is 'likely' to be used by a person named in an interception warrant. This may be particularly so in relation to personal computers that are open for public use (eg in public libraries or internet cafes). By way of contrast, a service-based named person warrant may well not authorise interception of all communications from such a device, as many of the users of such a device may not be using it to communicate via a service that the person named in the warrant is using or likely to use. Therefore, these amendments would increase the power of interception, and not merely establish an equivalence between device and service-based warrants.[41]

Legislative intent concerning device-based named person warrants

4.55 The Department expressed the view that the Bill 'clarifies' the original intent of the 2006 amendment bill to include multiple devices in a named person warrant. The Department stated that this is evidenced by the then inclusion of sections 16 and 60(4)[42] which appear to recognise that additional devices can be added to a warrant.[43]

---

41 *Submission* 8, pp 3-4.

42 *Committee Hansard*, 17 April 2008, p. 29 and as quoted in *Submission* 1, p. 8.

43 *Committee Hansard*, 17 April 2008, p. 29. *Submission* 1, p. 8.

The inconsistencies between these provisions are described in detail in Chapter 2 of this report.

4.56 The Department informed the committee that the inconsistencies were the result of a drafting error that, 'did not allow for the original policy intention for various devices to be added to a warrant'.[44]

4.57 A representative of the NSW Council for Civil Liberties observed that a change 'that requires 12 changes in the Act and changes to six of its clauses… is not merely carrying out the intentions of an original amendment.'[45]

4.58 The submission by the Law Council also disputed the legislative intent of the provisions, drawing attention to the Government response to the committee's inquiry into the 2006 amendment Bill, which stated that:

> These warrants will only be issued where the requesting agency can show that the unique identifying number is indeed a unique source and there are no other practicable methods of identifying the service.[46]

Conclusion

4.59 The committee disagrees with the argument presented by the Department that the Bill merely 'clarifies' the intent of the Telecommunications (Interception) Amendment Bill 2006 that a device-based named person warrant gives the authority to intercept multiple devices.

4.60 The inclusion of the conflicting provisions (described above and in Chapter 2) in the TIA Act indicates that it may well have been the Department's intent to incorporate multiple device provisions, including the ability to add devices to the warrant after the issue of the warrant. However, this cannot necessarily be used as an indication of the Parliament's intent when it passed the legislation, and indeed there is evidence to the contrary view, including:

- the committee's report on the 2006 Bill, which made it clear that there were substantive concerns with the ability to uniquely identify a telecommunication device and that these concerns related to protection of individual privacy and rights;
- the government's response to the committee's 2006 report, which also clearly indicated that a device-based named person warrant required the device to be identified in the warrant; and
- service-based and device-based named person warrants are to be clearly differentiated in terms of the nature and extent of their powers, with devices

---

44 *Committee Hansard*, 17 April 2008, p. 29.

45 *Committee Hansard*, 17 April 2008, p. 8.

46 Australian Government response, quoted from *Submission* 1, p. 9.

> requiring greater safeguards. This is evidenced by the TIA Act requiring an issuing authority to be satisfied that there are no other practicable methods available at that time to identify—or it is impracticable to intercept—the telecommunications services that the person of interest is using, before issuing a device-based named person warrant.

4.61 Arguments about the intent of the legislation are, in any case, futile. It is not disputed that currently, the TIA Act does not allow for multiple devices on a device-based named person warrant, or for devices to be added after the warrant has been issued. The objective of this Bill is to enable these changes, and the purpose of this inquiry is to assess their effects and advise the Senate accordingly.

Suggestions for safeguards if devices are added to warrants

4.62 During the course of this inquiry, privacy and civil liberties groups all clearly agreed that an application for multiple devices, identified in a device-based named person warrant, is appropriate. The committee questioned witnesses who had raised other concerns in relation to the Bill's proposed amendments about whether agencies should be able to apply for a warrant for multiple devices. None objected to multiple devices being included in a single warrant application.[47]

4.63 The Castan Centre explained that this was not objectionable in principle as:

> Currently, to intercept a new device, the agency would have to get a new warrant. If that was rolled into a process whereby, under the one warrant application and issuing process, they could identify and make the case for interception of multiple devices, I think that would be unobjectionable. That would in effect just be combining multiple processes into one process. There would be no reason to think that would interfere with the oversight and accountability in respect of each of those devices named.[48]

4.64 However, these groups informed the committee that the existing safeguards for telecommunication devices, as currently required by the TIA Act, should be maintained if devices are subsequently added to a warrant. The Law Council submitted that maintaining the status quo requires an issuing authority to be satisfied that a person is a legitimate target of suspicion and:

> For each and every device that-
>
> - the interception is likely to yield useful information (unobtainable by other means);
> - the device is used or likely to be used by the suspect; and
> - the device can be uniquely identified.[49]

---

47 *Committee Hansard,* 17 April 2008, pp 4, 8, 12 and 22 and Law Council, answer to question on notice, 17 April 2008 (received on 24 April 2008). Note that EFA was not asked this question.

48 *Committee Hansard,* 17 April 2008, p. 4.

49 *Submission* 1, pp 5-7.

4.65 Scrutiny of these issues by an issuing authority would enable an authority to adequately test how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant.

4.66 In a supplementary submission, the Privacy Foundation noted that its primary stance was to oppose a relaxation of the current issuing requirements for device-based warrants. However, the Privacy Foundation also put forward a model whereby an issuing authority would review additional devices within a short time-period, as follows:

> Agencies could be given an 'exceptional discretion' to intercept additional devices in relation to an existing named person warrant where timing or other operational circumstances made it impracticable to seek prior authorisation. However, exercise of this discretion would be subject to 'after the event' confirmation by an issuing authority, on presentation not only of the 'likely to be used' justification but also of the reasons for prior authorisation having been impracticable.
>
> Such an application for confirmation would be required within a fixed but short period after the interception of the additional device commenced. An issuing authority not persuaded by the case for the device could order immediate cessation of the interception….
>
> There is a clear precedent for this 'emergency authorisation' process in section 10 of the T(I&A) Act, which provides for the Director-General of Security to issue a warrant without the normal prior approval, subject to subsequent reporting to the Attorney-General and the Inspector-General.[50]

4.67 The Privacy Foundation also proposed a system of revocation and reprimand if the issuing authority was not persuaded by the case presented in the application for additional devices.

Proposed additional reporting of device-based warrant use

4.68 Part 2-8 of the TIA Act requires that the Attorney-General, as the Minister administering the TIA Act, prepare a report each year giving details of telecommunications interception for law enforcement purposes. The Department meets this requirement each year by publishing a consolidated report, the most recent of which is the *Telecommunications (Interception and Access) Act 1979, Annual Report for the year ending 30 June 2007.*

4.69 In relation to the need for additional safeguards if device-based warrant provisions are enacted, the Castan Centre's submission drew the committee's attention to the detail of current reporting requirements. These include, in relation to named person warrants issued during the year by each agency or authority, how many of those warrants involved the interception of:

- a single telecommunications service;

50 *Submission* 10a, p. 1.

- between two and five services;
- between six and ten services;
- more than ten telecommunications services; and
- the total number of telecommunication services intercepted under those warrants.

4.70 These requirements incorporate interceptions resulting from both device-based and service-based warrants, as the reporting is expressed in terms of the total number of services intercepted. There is no separate information provided in annual reports about the number or nature of devices intercepted.

4.71 The Castan Centre confirmed that the Bill is currently silent in terms of device-based reporting requirements and suggested that, were the proposed provisions for device-based warrants to be enacted, similar reporting to that in force for services should be required for device-based warrants, separately from service-based warrants. The Castan Centre argued that this would permit a degree of public scrutiny of the use to which the new power was being put.[51] Representatives of the Law Council supported the Castan Centre's view.[52]

4.72 EFA also supported the extension of reporting requirements to disaggregate device-based warrants. While considering this as a 'minimum', EFA argued that existing requirements are insufficiently detailed to allow scrutiny of the extent to which services additional to those identified in the original warrant application were intercepted. This point was illustrated in the following example:

> For example, one current reporting obligation is to report how many warrants 'involved the interception of more than 10 telecommunications services'. If a service-based named person warrant is issued, which identifies only one telecommunications service, and the agency involved intercepts a further 10 telecommunications services because they consider it 'likely' that the named person will use those services, would this warrant be reported as a warrant involving a single service, or more than 10 services?[53]

4.73 EFA submitted that there is a need for an additional reporting requirement to allow the disaggregation of services intercepted by services or devices identified in the original warrant, and those intercepted by services or devices subsequently added to the warrant. Additionally, this should be reported independently for service-based and device-based named person warrants. EFA considered that this is necessary because 'Statistics on this issue would indicate whether or not interception agencies might be overusing this power.'[54]

---

51 *Submission 8*, p. 7.

52 *Committee Hansard*, 17 April 2008, p. 12.

53 Answer to question on notice, 17 April 2008 (received on 22 April 2008), p. 1.

54 Answer to question on notice, 17 April 2008 (received on 22 April 2008), p. 1.

4.74 The committee sought a response from the representatives of the Department about the merits of this argument. Representatives confirmed that there is no additional reporting of the actual number of devices, but emphasised that the number of services intercepted under any device will still be reported in the annual report, as current reporting is on the number of services intercepted by all named person warrants:

> …regardless of the technology, whether it is done by device or service, it is the number of services that are intercepted that gives an indication of how many telecommunication services have been intercepted. The device is the technology by which the interception takes place.[55]

4.75 When asked to do so by the committee, the Departmental representative said that she was unable to comment on the merits of a specific reporting requirement for device based warrants, '…given that I believe the information is already in the reporting'.[56]

Balance of probabilities test

4.76 EFA submitted to the committee that the term 'likely' (as discussed in chapter 2, commencing at 2.16) was too open to interpretation in relation to a suspect 'using or likely to use' each device from which communications will be intercepted. The EFA stated:

> …the standard of a 'real chance or possibility' would be unacceptably low, and would both encourage and facilitate fishing expeditions by agencies with interception powers. These fishing expeditions could result in the interception of telecommunications devices belonging to a suspect's friends, relatives or workmates, not because the agency concerned believes that the suspect *will* use those devices, but merely because they *might*.[57]

4.77 A representative of the EFA told the committee that the word 'likely' is unclear, and is given various meanings by different courts, considering different legislation at different times. He said the meaning can range from the balance of probabilities, as in 'more likely than not', as a layperson would interpret it, to the low standard of a real chance or possibility. He stated that a balance of probabilities test is required.[58]

4.78 The committee asked the Department whether it would consider a balance of probabilities test. The Department's response was that it considered that the phrase 'likely to use' is an appropriate test:

---

55 *Committee Hansard*, 17 April 2008, p. 29.

56 *Committee Hansard*, 17 April 2008, p. 29.

57 *Submission*, p. 2.

58 *Committee Hansard*, 17 April 2008, p. 18.

> The 'likely to use expression in section 46A provides a mechanism that enables intelligence gathering where something is likely to occur in the future. Human action is difficult to predict. However, in the context of the TIA Act, the term 'likely' should be interpreted as being analogous with a 'real risk'[59] or 'probable[60] that the named person is using or likely to use a device. To satisfy such a test would require evidence as to why an agency suspects that a person is likely to use a device.[61]

Discarding of data from persons not named in the warrant

4.79 On being questioned by the committee on additional safeguards that would limit surveillance of non-suspects in device-based warrants, a representative of EFA suggested that it could be a requirement that all communications that were not made by the person named in the warrant be discarded. The representative went on to state that it was EFA's understanding that:

> … under the law as it currently stands, the communications of those persons can be recorded and are only discarded if they are not really relevant to a crime which is investigated by that type of agency….It says on page 4 of the A-G's [Attorney General's] submission:
>
> - Intercepted material must be destroyed where it is not relevant to the permitted purposes of the agency—generally an investigation of an offence that is punishable by three years imprisonment or more.[62]

4.80 A representative of the Department responded to the committee's questions on the secondary use of data stating that there are no legislative provisions relating to the collection of interception data for general intelligence, no centralised database for its storage and that it is an offence to disclose intercepted information, except for the permitted purposes for which it is obtained. The representative stated that:

> There is no derivative use of TI [telecommunications interception] product except for those very limited grounds which are in the Act, and that is for the permitted purpose of the original investigation or to pass it over for a relevant offence, which has to be punishable by at least three years imprisonment. So it is very, very tightly guarded. Certainly the AFP can talk more about their destruction provisions, but each intercepting agency has very strong accountability regimes inside such that they do have to destroy, and it is part of the role of those oversight bodies like the Ombudsman that they review and make sure that that has actually been

---

59 Secretary, Department of Employment, Education, Training Youth Affairs v Suzanne Barrett & Anor (1998) 82 FCR 524, in Attorney General's Department, answer to question on notice, 17 April 2008 (received on 24 April 2008), p. 1.

60 Australian Telecommunications Commission v Krieg Enterprises Pty Ltd (1976) 14 SASR 303 at 309-313, in Attorney General's Department, answer to question on notice, 17 April 2008 (received on 24 April 2008), p. 1.

61 Answer to question on notice, 17 April 2008 (received on 24 April 2008), p. 1.

62 *Committee Hansard*, 17 April 2008, p. 19.

> undertaken. And, if not, then reports are made to ministers that they have breached their obligations to destroy particular information.[63]

4.81 The committee notes that the offence threshold for the secondary use of data appears to be less restrictive, than that which applies when an issuing authority considers a device-based named person warrant application. For example, the Department's submission stated that an issuing authority for such a warrant would need to be satisfied that:

> … the interception is for an investigation of a serious offence, generally punishable by a maximum period of imprisonment of at least seven years.[64]

Committee findings

4.82 The committee considers it desirable that an issuing authority should be able to approve multiple devices identified in a device-based named person warrant application and add additional identified devices to that warrant at later stages.

4.83 The committee considers that the process of adding a device to a device-based named person warrant after the warrant has been issued should include an independent scrutiny process. The committee considers that the model proposed by the Australian Privacy Foundation, discussed at paragraph 4.66, provides a useful starting point.

4.84 The committee considers that the annual report on the TIA Act is reasonably comprehensive in terms of providing a breakdown of interceptions that have taken place and the agencies undertaking the interceptions. However, it is also important for the Parliament to be able to discern the effects of any new legislation and accordingly, the committee is of the view that additional reporting of the use of these powers is required.

4.85 The committee considers that the number of services intercepted by service-based and device-based named person warrants should be disaggregated, and the results presented in a similar manner to that currently for intercepted services. The committee also considers that the number of services intercepted pursuant to the services or devices in the original application should be reported separately to the services intercepted by later additions to the warrant. This should be reported separately for device-based and service based named person warrants in a similar manner to that currently used for the reporting of intercepted services.

---

63 *Committee Hansard*, 17 April 2008, p. 30.

64 *Submission* 7, p. 3.

Recommendation 2

4.86 The committee recommends that the recommendation at paragraph 3.2.5 of the Blunn report, which reads:

> **3.2.5. Accordingly, I recommend that priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access.**

be adopted, and priority given to developing a unique and indelible identifier of the source of telecommunications.

Recommendation 3

4.87 The committee recommends that the Bill be amended to provide that an agency be permitted to add a device to a device-based named person warrant after the warrant has been issued if the facts of the case would have justified the issue of a warrant by the issuing authority; and the investigation in relation to the person named in the warrant will be, or is likely to be, seriously prejudiced if the interception does not proceed.

Recommendation 4

4.88 The committee further recommends that the Bill be amended to provide that if an agency adds a telecommunications device or devices not identified on a device-based named person warrant at the time that the issuing authority issued the warrant:

(i) the agency be required to notify an issuing authority, within 2 working days, that a device had been added to the warrant; and

(ii) the issuing authority must examine the supporting documentation against the criteria that it would have considered, in accordance with the requirements of the *Telecommunications (Interception and Access) Act 1979*, in relation to an application by the agency for a device-based named person warrant, and make a determination about whether the facts of the case justified the addition of the device; and

(iii) the issuing authority shall order that the interception cease immediately and that all evidence gathered be destroyed if it determines that the facts of the case would not have supported the issue of a device-based named person warrant.

Recommendation 5

4.89 The committee recommends that the Bill be amended to insert a requirement that the Annual Report in relation to the *Telecommunications (Interception and Access) Act 1979* incorporate the following additional information over and above that already required by the Act:

- **the number of service-based and device-based interceptions, to be reported upon separately but in a similar format to that currently used for the total number of intercepted telecommunication services; and**

- **the number of devices in the original warrant and the number of additional devices added to the warrant, reported in a similar format to that currently used for reporting the total number of intercepted telecommunications services.**