Electronic Frontiers Australia Inc

PO Box 382 North Adelaide
SA 5006 AUSTRALIA
www.efa.org.au
email@efa.org.au
Tel: 07 3424 0201
Fax: 07 3424 0241

3 June 2004

Briefing Paper: *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*

Overview

The *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*, introduced into the House of Representatives on 27 May 2004, is the Commonwealth Government's third attempt since early 2002 to amend the *Telecommunications (Interception) Act 1979* in relation to email, SMS and voice mail messages.

The first Bill, introduced in March 2002, sought to remove the protection from interception for delayed access messages. Those provisions were deleted by the government when it became clear they did not have sufficient support in the Senate. The second Bill, introduced in February 2004, sought to increase the protection for delayed access messages. Those provisions were deleted due to disagreement between the Attorney−General's Department (relying on the opinion of the Solicitor−General) and the Australian Federal Police (relying on the opinion of the C'th Director of Public Prosecutions) concerning the correct interpretation of the law.

The third (current) Bill, introduced in May 2004, not only reverts to substantially the same proposal as was rejected in 2002, but would remove even more of the existing protections from interception than the 2002 Bill would have.

The Bill would inappropriately change the long−established balance in telecommunications interception law between individuals' right to privacy and the needs of law enforcement agencies.

Under current law, an interception warrant is required to access the contents of email, SMS and voice mail messages that are temporarily delayed and stored during passage over the telecommunications system, (e.g. stored on an ISP's or telephone service provider's equipment pending delivery to the intended recipient), the same as is required to intercept a telephone call.

The Bill would remove the existing protection from interception for email, SMS and voice mail messages that have not been delivered to the intended recipient, thereby allowing government agencies (not only police), private investigation agencies, telephone companies and ISPs and other businesses to access such communications, without a warrant of any type.

Although the Commonwealth Government frequently cites enthusiasm for "technology neutral" laws, this Bill is certainly not. It treats email, SMS and voice mail telecommunications quite differently from facsimile and telephone call telecommunications.

Detailed Briefing Paper

Contents

Executive Summary

- The effect of the Bill is substantially the same as the rejected 2002 proposal. However, it is even more objectionable than the 2002 proposal because it completely removes email, SMS and voice mail messages (stored communications) from the scope of the *Telecommunications Interception Act 1979* ("the TI Act"). This results in serious issues additional to the highly controversial aspects of the rejected 2002 Bill:

    - ♦ It would no longer be an illegal interception if a person (whether an LEA officer or any other person) down loaded someone else's email, or dialed into their voice mail box to listen to their messages without their knowledge. (Such interception would have remained illegal under the 2002 Bill.)

    - ♦ It would no longer be an illegal interception if employees of telephone companies and ISPs intercepted and spied on their customers' undelivered email, SMS and voice mail messages. The existing protections in that regard were enacted in 1995 in direct response to the Casualties of Telecom cases ("CoT cases") following the AUSTEL inquiry finding that Telecom had intercepted and taped customer telephone calls. (Such interception would have remained illegal under the 2002 Bill.)

- Access to undelivered email, voice mail, SMS, etc messages would become available to criminal and civil law enforcement agencies not only with a search warrant, but also without a warrant of any type (as detailed later herein).

- Even if the Bill or the *Telecommunications Act 1997* was amended to require a search warrant to access delayed communications stored on telecommunications service providers' equipment, the longstanding, rigorous safeguards and controls set out in the *Telecommunications Interception Act 1979* to prevent misuse of the power to intercept do not apply to search/seizure warrants issued to various Commonwealth, State and Territory agencies.

- Some State/Territory police forces would gain a new right to snoop. Some are not authorised to obtain interception warrants under the TI Act because the relevant Government and/or Parliament has not implemented the necessary complementary legislation imposing parallel supervisory and accountability provisions, including those relating to inspection and reporting requirements. Police in such jurisdictions would gain the new right to intercept messages temporarily delayed and stored during transit. According to the 'Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2003', only the police forces of Victoria, NSW, South Australia and Western Australia (and some crime/anti−corruption Commissions in NSW and WA) have been authorised to obtain interception warrants.

- Agencies other than criminal law enforcement agencies, that are not authorised to use interception warrants, would be able to access the content of undelivered stored communications on service providers' equipment, i.e. access information that they presently have no power to access. This includes agencies such as the Australian Taxation Office, Australian Securities & Investment Commission (ASIC), Australian Transaction Reports and Analysis Centre (AUSTRAC), Australian Customs Service, Immigration Department, etc.

- Private organisations such as lawyers representing copyright holders would gain a right to snoop through communications that have been delayed and temporarily stored during transit

when executing a secretly issued civil search order, known as an Anton Pillar order, at the premises of ISPs and universities etc. A number of such privatised searches have been conducted in Australia during the past twelve months but access to communications in transit would have been prohibited by the TI Act. The Bill would remove the prohibition.

- A search warrant affords considerably less privacy protection than does the current requirement of an interception warrant:

    - ♦ Less strict requirements govern issue of search warrants than interception warrants. The conditions of issue of interception warrant set out in the TI Act that aim to ensure privacy of non−suspect third parties is not unduly infringed do not apply to ordinary search warrants.

    - ♦ Interception warrants can only be issued by eligible judges and nominated members of the Administrative Appeals Tribunal. Search warrants can be issued by less appropriately qualified persons, including some likely to be biased against giving adequate consideration to privacy issues, such as police officers, officers of government departments, justices of the peace, etc.

    - ♦ Limitations set out in the TI Act on the secondary (subsequent) disclosure and use of information obtained from execution of an interception warrant do not apply to information obtained under a search warrant, or without a warrant of any type.

    - ♦ Agencies would be able to obtain access, without an interception warrant, to the content of stored communications on service providers' equipment when investigating a significantly broader and far less serious range of suspected offences than the specified serious criminal offences permitted under the TI Act.

- Enabling government agencies and private organisations to access undelivered communications stored on service providers' equipment in effect results in secret surveillance that is vastly more open to abuse than are search warrants executed on a suspect's premises. When an individual's home or office is raided by police, the individual is in a position to report such an event to the relevant ombudsman if they believe the search should not have been conducted. This minimises the prospect of police and agencies misusing search powers. It is very unlikely that service providers would inform their customer that a search of his/her communications had been undertaken by police or another agency. While this situation also applies to interception warrants, the TI Act contains rigorous safeguards and controls designed to prevent misuse.

- Since early 2002, patches to the existing legislation have been tried twice by the government. The currently proposed third patch is even more problematic than the first version. The existing TI Act should remain in place unamended for the forthcoming 12 months, while the Attorney−General's Department conducts the announced full review of the interception legislation.

- The *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* should be abandoned. The Bill is an utter disgrace. It is the type of legislation one might expect to see in a police state, not in a democracy.

Background

The Existing Law

Currently, the *Telecommunications (Interception) Act 1979* prohibits interception of communications passing over a telecommunications system, except when authorised by an interception warrant. Law enforcement agencies are not permitted to access the content of messages (such as email, voice mail, SMS, etc) that are temporarily stored on a telecommunications service provider's equipment during transit, unless they have obtained an interception warrant.

After a message has been delivered to the intended recipient (i.e. has completed its passage over the telecommunications system) law enforcement agencies can lawfully access the content of the message with a search or seizure warrant. Such a warrant may cover the recipient's equipment (e.g. computer containing down loaded email, mobile phone SIM card, etc) or the service provider's equipment when a copy of the message remains on their equipment.

The 2002 Bill

The *Telecommunications Interception Legislation Amendment Bill 2002* ("the 2002 Bill") was one of a suite of anti−terrorism Bills, named the *Security Legislation Amendment (Terrorism) Bill 2002 [first 2004 Bill] and Related Bills*.

Prior to its introduction, statements by the then Attorney−General and the National Crime Authority on the provisions of existing law included:

- Media release issued by Attorney−General Daryl Williams, 18 December 2001:
  "At present, an agency with a valid search warrant cannot access e−mail communications unless they have been read, or otherwise consciously dealt with, by the intended recipient. The Telecommunications (Interception) Act 1979 will be amended to permit access to unread e−mails where another form of lawful access to the system or device capable of displaying the communication is held by the relevant agency."
- Parliamentary Joint Committee on the National Crime Authority Report on the Law Enforcement Implications of New Technology, August 2001. Paragraph 1.80 of Committee's report states the NCA said in its submission to the inquiry that:
  "A sent but unopened email needs a TI warrant for interception. Once the email has been down loaded and opened by the recipient it is their property and a search warrant is required. This also applies to Short Message Services (SMS) and voice messages stored in remote locations."

The 2002 Bill (within the package of security Bills) was referred to the Senate Legal and Constitutional Legislation Committee for inquiry on 20 March 2002 and the Committee issued its report on 8 May 2002. In relation to the 2002 Bill, the Committee recommended:

> "Recommendation 5
> The Committee recommends that the Attorney−General review the current law on access to stored communications of delayed messages services with a view to amending the Telecommunications Interception Legislation Amendment Bill 2002 so that the accessing of such data requires a telecommunication interception warrant."

As reported in an article titled '*Email snooping loses vote*' (*The Australian IT*, 2 July 2002) the Bill:

> "... sought to give government agencies the power to intercept and read messages without an interception warrant. A warrant would have remained necessary to tap telephone calls.
> ...
> Labor IT spokeswoman Kate Lundy said it was unacceptable for 'stored telecommunications' − email, SMS and voice mail − to receive less privacy protection than telephone calls.
> 'It's almost a loophole in the telecommunications process by virtue of the fact that emails get stored on a server, and the Government was trying to exploit that,' she said."

Subsequently, the stored communications provisions were deleted from the 2002 Bill during its passage through the Senate. The ALP and the Democrats had made clear to the government that they opposed the amendments and would not support them.

Senator Faulkner (Leader of the Opposition in the Senate) remarked in the Senate on 27 June 2002:

> "Of the whole terrorism package that the parliament has dealt with, these [stored communication provisions] are amongst the most controversial provisions contained in that package. ... the opposition will be opposing the proposal that these parts of the bill stand as printed. I support removing the provisions, which means I am going to vote against the question before the chair".

In the House of Reps later on 27 June 2002, Mr Melham MP remarked that:

> "It should also be noted that, at the opposition's insistence, the government has removed its controversial proposal for easier access to emails and SMS messages from its proposed amendment of the Telecommunications (Interception) Act."

The government said it would re−introduce amendments concerning stored communications at a later date.

The First 2004 Bill

On 19 February 2004, two years after rejection of the 2002 proposal, the *Telecommunications (Interception) Amendment Bill 2004* ("the First 2004 Bill") was introduced into Parliament. This Bill was the opposite of the government's 2002 proposal. It provided improved protection for stored communications by extending the definition of "interception" to include reading or viewing a communication, thereby providing increased privacy protection for text based communications, such as email and SMS messages. It also sought to clarify the existing law to ensure it is clear that law enforcement authorities are required to obtain an interception warrant before accessing communications temporarily delayed and stored during passage.

On 3 March 2004, the First 2004 Bill was referred to the Senate Legal and Constitutional Legislation Committee for inquiry and report by 30 March 2004.

During the Committee's inquiry it became apparent that government agencies disagree, and so do the Solicitor−General and Commonwealth Director of Public Prosecutions ("CDPP"), on the correct interpretation of the existing law and how it would operate under the proposed amendments. The Australian Federal Police ("AFP"), relying on the opinion of the CDPP, said they believe they are

currently allowed to intercept communications temporarily stored on telecommunications service providers' equipment without an interception warrant due to the operation of the general search powers in Section 3L of the Crimes Act. (Section 3L came into effect with the Cybercrime Act 2001 which was rushed through Parliament in the wake of September 11.) However the Attorney−General's Department, relying on the advice of the Solicitor−General, said Section 3L does not over−ride the Telecommunications Interception Act, that is, the AFP is currently required to obtain an interception warrant.

The Committee issued its report on 30 March 2004 and, in relation to the stored communications provisions, recommended:

> "Recommendation 1
> The Committee recommends that Parliamentary consideration of proposed subsections 6(1) 6(5), 6(6) and 6(7) be deferred until Parliament is informed of agreement between the Attorney−General's Department and the AFP on the current operation of the TI regime, and how it will operate under the Bill."

Following the Committee's recommendation, the government deleted the stored communications provisions from the Bill.

Subsequently, the government's third attempt to amend the Act in relation to stored communications was introduced in May 2004 and is discussed below.

The Current 2004 Bill: *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*

The effect of the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* ("the Current 2004 Bill") is substantially the same as the rejected provisions in the 2002 Bill. However, this Bill would make access to undelivered communications even more easily available to law enforcement agencies than did the 2002 proposal because it completely removes stored communications from the scope of the TI Act. In addition, the Bill would make access available to other people including private investigation agencies, telephone companies, ISPs and other businesses.

The Attorney−General's media release of 27 May 2004 states:

> "...the amendments will enable access to stored communications, such as email and voicemail, without a telecommunications interception warrant.
> The amendments will allow access to stored communications under other forms of lawful authority, such as a search warrant".

The same was said about the 2002 Bill. For example, on 19 April 2002, the Attorney−General's Department informed the Senate Committee hearing that agencies would be permitted to access stored communications "under some other lawful authority like a search warrant".

The Current 2004 Bill, like the 2002 Bill, would remove the need for an interception warrant to access the content of communications temporarily delayed and stored on a telecommunication service provider's equipment during transit. As a result, access to undelivered email, voice mail, SMS, etc messages would become available not only with a search warrant, but also without a warrant of any type (as detailed later herein).

Analysis & Issues

1. Less privacy protection than in rejected 2002 Bill

Although the Current 2004 Bill is substantially the same as the 2002 proposal, it is even more objectionable than the 2002 proposal because, unlike the 2002 Bill, it completely removes email, SMS and voice mail messages (stored communications) from the scope of the *Telecommunications Interception Act* ("the TI Act"). This results in serious issues additional to the highly controversial aspects of the 2002 Bill as discussed below.

1.1 Accessing another person's undelivered messages would cease to be an illegal interception

The existing TI Act makes it an offence for a person to "(a) intercept; (b) authorize, suffer or permit another person to intercept; or (c) do any act or thing that will enable him or her or another person to intercept; a communication passing over a telecommunications system" (s7(1)) "without the knowledge of the person making the communication" (s6(1)).

The 2002 Bill deemed a stored communication to no longer be passing over the telecommunications system when it can be accessed on the equipment on which it is stored, but without using a telecommunications line. The Bill contained the following examples:

> "Example 1: An e−mail is a stored communication if it has been down−loaded from a service provider onto a computer and can be accessed using that computer without any further use of a line.
>
> Example 2: A voicemail message is not a stored communication if it can only be accessed by dialling a number."

The Current 2004 Bill does not define a stored communication in the above way. It merely states that "a stored communication is a communication that is stored on equipment or any other thing" and removes such communications from the scope of the TI Act. In that regard, the Bill specifically provides that the existing s7(1) prohibition on interception of communications in transit "does not apply to or in relation to ... (ad) the interception of a stored communication".

As a result, if the Current 2004 Bill is enacted, it would no longer be an illegal interception if a person (whether an LEA officer or any other person) down loaded someone else's email, or dialed into their voice mail box to listen to their messages without their knowledge.

It appears the above situation results from the government having apparently decided to seek to grant the Australian Federal Police's wish that they be permitted to remotely access stored communications under Section 3L of the Crimes Act instead of needing to obtain an interception warrant. Irrespective of whether the Parliament considers there is any merit in granting the AFP's wish, the Parliament must not allow the government to use that as an excuse or justification for removing, as proposed, all protection from interception so that anyone, not only the AFP, is permitted to intercept stored communications.

1.2 Re−enables telco employee spying like in Casualties of Telecom cases

The Current 2004 Bill also removes the existing protection in the TI Act which prohibits employees of telecommunications service providers from spying on customers' electronic communications during their passage.

The existing protection in that regard was enacted in 1995 in direct response to the Casualties of Telecom cases ("CoT cases") following the AUSTEL inquiry finding that Telecom had intercepted and taped customer telephone calls. Section 7(2) of the TI Act was amended to tighten up the exceptions to the prohibitions on interception by a carrier employee, so that such interception is only permitted "where it is reasonably necessary for the employee [to do so] in order to perform [his/her] duties effectively". More information about those 1995 amendments is contained in Senate Legal and Constitutional Legislation Committee's Report on the Telecommunications (Interception) Amendment Bill 1995.

Removing those restrictions would obviously be contrary to the Parliament's intention in 1995. However, it is plainly the government's intention in relation to temporarily delayed and stored communications as stated in the Explanatory Memorandum:

> "The practical effect of the new provisions inserted by items 3 and 4 is that it will no longer be necessary to obtain a telecommunications interception warrant, or to rely on another exception to the prohibition against interception, in order to intercept a stored communication. The amendments allow for a stored communication to be intercepted by a person having lawful access to the communication or the equipment on which it is stored. A person may have lawful access to a communication, for example, ... in the person's capacity as a network owner or administrator."

It appears the above situation results from the Australian Federal Police having argued that if the stored communications provisions of the First 2004 Bill had been enacted, the AFP's IT staff would be prohibited from reading suspect email arriving on the AFP's mail server to see if it was spam or contained a virus etc before allowing it to be sent on to the intended recipient. However, that issue arose because the First 2004 Bill would have extended the definition of interception to include viewing and reading.

While the AFP and other employers may have a legitimate need to be able to control/prevent spam etc being received by all their staff, the Parliament must not allow that to be used as an excuse or justification for removing all existing protections from interception. There is a vast difference between allowing employers to manage their private internal systems and allowing telecommunications servicer providers' employees to have unfettered access to trawl through their customers' temporarily delayed and stored communications without the customer's knowledge and permission.

2. Same issues and problems as in rejected 2002 Bill

2.1 No warrant of any type would be required to access communications delayed in transit

The Attorney General's recent media release and second reading speech (like statements made regarding the 2002 Bill) suggest it would be necessary for LEAs to obtain a search warrant, instead of an interception warrant, to access the content of communications temporarily delayed and stored during transit.

However, access to such communications would become available without a warrant of any type under existing provisions of the *Telecommunications Act 1997* such as Section 280(1)(b) and quite possibly Sections 282(1) and (2).

While currently the above provisions may apply to stored messages that have completed their passage over a telecommunications system, they do not apply to messages that are temporarily delayed and stored during their passage. This is because the requirement for an interception warrant under the *Telecommunications Interception Act* to access messages during their passage over a telecommunications system over−rides the provisions of the *Telecommunications Act*. However, if the Current 2004 Bill is enacted, the prohibition on disclosing content of messages delayed during passage (unless an interception warrant has been obtained) will cease.

Section 280

The content of temporarily delayed and stored communications would become available under s280 of the *Telecommunications Act 1997*. For example, s280(1)(b) permits disclosure or use of information or a document if that is required or authorised by or under law. This broad term includes statutory, judicial and quasi−judicial powers, such as court orders made during the discovery process, summons for witnesses to attend and produce records and subpoenas for documents. Further, as stated in the ACA's Telecommunications and Law Enforcement Manual:

> "Section 280 covers the situation of disclosures being authorised or required under another law ... Some agencies, both criminal law enforcement and other enforcement agencies, operate under special legislation which gives them a right to access information. The operation of this legislation might allow for the issue of ... instruments such as 'notices to produce'."

Section 282

In addition, Sections 282(1) and (2) of the *Telecommunications Act* permit carriers and carriage service providers (including ISPs) to disclose documents and information to agencies on request (without a warrant or even written certified request) if the service provider considers the disclosure or use is "reasonably necessary" for the enforcement of the criminal law (s282(1)), or the enforcement of a law imposing a pecuniary penalty, or the protection of the public revenue (s282(2)).

The Attorney−General's Department acknowledged the possibility of access to the content of communications under Section 282(1) and (2) of the *Telecommunications Act* (i.e. without a warrant of any type) in their 1999 Report titled *Telecommunications Interception Policy Review* and this aspect of the *Telecommunications Act* has not been amended since 1999. The Report states:

> "Section 4.3 − Access to stored data
> ...
> 4.3.11 Access by enforcement agencies to information held by C/CSPs [under the Telecommunications Act] is by means of two primary mechanism, certified and uncertified requests.
>
> 4.3.12 Subsection 282(6) of the Telecommunications Act provides that the certificate provisions in subsections 282(3), (4) and (5) do not apply to the contents of a communication whether or not the communication has been received by the intended recipient.
>
> 4.3.13 However, this still leaves the possibility that subsections 282(1) and (2) can apply in respect of the content of stored communications. That is, an enforcement agency (including civil penalty−enforcement and public revenue protection agencies) could get access to the contents of a stored communication if the disclosure of the stored communication is reasonably necessary for one of the purposes listed in subsections 282(1) and (2).
>
> 4.3.14 The draft ACIF Assistance to Enforcement Agencies Code has had to address this issue. ... Currently Clause 2.7.2 says−
> 'S282(1) and (2) may authorise disclosure of content and substance. In view of the sensitive nature of the disclosure where content and substance are involved it would be prudent for Organisations (that is carriers and carriage service providers) to obtain legal advice. ...' "
>
> [Note: The same Clause 2.7.2 was contained in final industry code issued in 2001 − ACIF C537:2001.]

The uncertainty concerning s282(1) and (2) is also apparent in documents issued by the Australian Communications Authority ("ACA"). The ACA's Fact Sheet *Internet Service Providers and Law Enforcement and National Security* states:

> "What about stored communications?
> Access to the content of communications (for example, electronic mail) stored on an ISP's server is unlikely to fall within reasonably necessary assistance [i.e. s282(1) and (2)]. An agency may use a general search or interception warrant or some other statutory provision to access stored communications."

That the ACA is only able to say "unlikely" demonstrates that they, like the Attorney−General's Department, recognise the possibility that subsections 282(1) and (2) might apply in respect of the content of stored communications. Obviously the *Telecommunications Act* is insufficiently clear to ensure protection of the contents of communications from access without a warrant.

Section 282 is very frequently used to obtain call charge records etc. It enables disclosure of information such as customer identification details and the source, path and destination of communications (for example, telephone numbers dialled, and the "To" and "From" fields of an email message, etc). In the 2002−2003 year, 400,766 disclosures of information or documents were made to government agencies under s282(1) and (2) of the *Telecommunications Act* (i.e. without a warrant or certificate) by telecommunications carriers, carriage service providers (includes ISPs) or number database operators. This is 60% of the total disclosures (666,521) under Part 13 of that Act. (Source: ACA Annual Report)

No doubt the agencies who made the requests for nearly half a million disclosures would like to be able to obtain the content of communications temporarily delayed in transit under the same provisions. It is highly disturbing that this might be possible if the Current 2004 Bill is enacted.

2.2 Comparison of Search Warrants and Interception Warrants

Search warrants are subject to markedly less safeguards and are less protective of citizens' privacy than interception warrants

Even if a Bill to amend the *Telecommunications Act 1997* was enacted to ensure a search warrant would be required to access content of communications stored during transit, a search warrant affords considerably less privacy protection than does the current requirement of an interception warrant.

Moreover, the longstanding, rigorous safeguards and controls set out in the *Telecommunications Interception Act* to prevent misuse of the power to intercept do not apply to search/seizure warrants issued to various Commonwealth, State and Territory agencies.

For example:

- **Less strict requirements govern issue of search warrants than interception warrants.** The eligible judges and nominated members of the Administrative Appeals Tribunal who are authorised to issue interception warrants must comply with conditions of issue set out in the TI Act that are intended to ensure privacy is not unduly infringed. Applicants for interception warrants are required to demonstrate that the information likely to be obtained from the interception will materially assist the investigation, that there are no alternative methods available (or that they have been tried without significant success), and that in the case of 'Class 2' offences that the matter is sufficiently serious to justify intrusion into individuals' privacy.

  Issue of search warrants is not subject to such conditions and can be issued by less appropriately qualified persons, including some likely to be biased against giving adequate consideration to privacy issues, such as police officers, officers of government departments, justices of the peace, etc.

- **Removal of existing restrictions on secondary disclosure and use of content of intercepted communications.** Limitations set out in the TI Act on the secondary (subsequent) disclosure and use of information obtained from execution of an interception

warrant do not apply to information obtained under a search warrant, or without a warrant of any type.

- **Access no longer restricted to the investigation of serious criminal offences**.
  Agencies would be able to obtain access, without an interception warrant, to the content of stored communications on service providers' equipment when investigating a significantly broader range of suspected offences than is permitted under the TI Act.

  Interception warrants can only be issued in relation to the investigation of a "serious offence" i.e. Class 1 and Class 2 offences specified in the TI Act. In most instances it is a requirement that the offence be punishable by imprisonment for life or for a period of at least 7 years. Class 1 offences include conduct involving an act or acts of terrorism, murder, kidnapping, narcotics offences and being a party to those offences. Class 2 offences include those which are punishable by a maximum of at least seven years imprisonment and involve for example, loss or serious risk of loss of a person's life; serious personal injury or serious risk of same; serious damage to property in circumstances endangering the safety of a person; serious arson; serious fraud, drug trafficking, bribery and corruption of or by government officers, dealing in child pornography; procuring a child in connection with child pornography; money laundering; people smuggling with exploitation, slavery, sexual servitude and deceptive recruiting; specified cybercrime offences; and also offences involving two or more offenders and substantial planning and organisation of a kind involving the use of sophisticated methods and techniques in relation to specified crimes such as theft, fraud, extortion; harbouring criminals; dealings in firearms or armaments; a sexual offence against a person who is under 16; an immigration offence.

  While the above list is quite extensive, search warrants can be issued for many more reasons and purposes than can interception warrants.

- **Some State/Territory police forces would gain a new right to snoop.**
  The police forces of some States/Territories are not authorised to obtain interception warrants because the relevant Government and/or Parliament has not implemented the necessary complementary legislation. Interception warrants can only be issued to agencies that are specifically authorised under the TI Act (e.g. the Australian Federal Police and the Australian Crime Commission) and 'declared agencies' under s34 of the TI Act. According to the 'Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2003', only the police forces of Victoria, NSW, South Australia and Western Australia (and some crime/anti−corruption Commissions in NSW and WA) had been declared.

  Before the C'th Attorney−General can declare a State agency, there must be State legislating complementing the Commonwealth *Telecommunications (Interception) Act 1979*. State legislation must impose parallel supervisory and accountability provisions, including those relating to inspection and reporting requirements, on the State authority. Hence, police forces and other agencies of States that are not bound by such complementary legislation are not and cannot be authorised to obtain interception warrants.

  Generally, issue of search warrants is not subject to equivalent supervisory and accountability provisions and, as outlined earlier herein, a search warrant would not necessarily be required in any case.

  Enactment of the Current 2004 Bill would no doubt be a wish come true for police forces and agencies in States where the Government and/or Parliament has not enacted complementary legislation. They would become allowed to access, under an unaccountable

regime, communications delayed during transit that they are not currently permitted to access.

- **Secret surveillance facilitates police and other agency misuse of power.**
  Enabling agencies to access undelivered communications stored on service providers' equipment in effect results in secret surveillance that is vastly more open to abuse than are search warrants executed on a suspect's premises. When an individual's home or office is raided by police, the individual is in a position to report such an event to the relevant ombudsman if they believe the search should not have been conducted. This minimises the prospect of police and agencies misusing search powers. It is very unlikely that service providers would inform their customer that a search of his/her communications had been undertaken by police or another agency.

- **Broader range of agencies would be permitted to snoop.**
  Agencies other than criminal law enforcement agencies, including agencies that are not authorised to use interception warrants, would be able to access the content of undelivered stored communications on service providers' equipment, i.e. access information that they presently have no power to access. This includes agencies such as the Australian Taxation Office, Australian Securities & Investment Commission (ASIC), Australian Transaction Reports and Analysis Centre (AUSTRAC), Australian Customs Service, Immigration Department, etc.

- **Private investigation agencies would gain new right to snoop.**
  Private organisations such as lawyers representing copyright holders would gain a right to snoop through communications that have been delayed and temporarily stored during transit when executing a secretly issued civil search order, known as an Anton Pillar order, at the premises of ISPs and universities etc. A number of such privatised searches have been conducted in Australia during the past twelve months but access to communications in transit would have been prohibited by the TI Act. The Current 2004 Bill would remove the prohibition.

Conclusion

The *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* should be abandoned. The Bill is an utter disgrace. It is the type of legislation one might expect to see in a police state, not in a democracy.

In addition to the matters raised earlier herein, the Bill fails to recognise that interception of communications invades the privacy of third parties who have nothing to do with the police investigation.

Allowing access to the telecommunications of people who are not even suspected of engaging in crime, without a warrant, or even with an ordinary search warrant designed for searching for property, fails to give due regard to Australia's obligations as a party to the International Covenant on Civil and Political Rights (ICCPR). Article 17 of the ICCPR provides:

> (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> (2) Everyone has the right to the protection of the law against such interference or attacks.

Although the government claims the proposed amendments are "urgent", it should be noted that this claim was also made when the 2002 Bill was introduced in the package of anti−terrorism Bills. Nevertheless, after the 2002 stored communications provisions were rejected, the government did not introduce its next proposal until two years later. Clearly the amendments were not urgent in 2002 and no evidence has been put forward to demonstrate that the amendments are urgent now.

The existing Act should remain in place unamended for the forthcoming 12 months, while the Attorney−General's Department conducts the announced full review of the interception regime.

References

1. *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*
    - ♦ Text of Bill (PDF 13 Kb)
    - ♦ Explanatory Memorandum (PDF 16 Kb)
    - ♦ Minister's Second Reading Speech
2. *Telecommunications (Interception) Amendment Bill 2004*
    - ♦ Text of Bill
    - ♦ Explanatory Memorandum
    - ♦ Bills Digest No. 111 (prepared by the Parliamentary Library)
    - ♦ Senate Legal and Constitutional Legislation Committee Inquiry into the *Telecommunications (Interception) Amendment Bill 2004*:
        - ◊ Committee Report and Recommendations, 30 March 2004
        - ◊ Hansard Transcript of Committee hearing, 22 March 2004 (Witnesses: EFA, Australian Federal Police and the Attorney−General's Department)
        - ◊ EFA Submission to Inquiry
        - ◊ Other Submissions to Inquiry (incl. Australian Privacy Foundation, Victorian Privacy Commissioner, Attorney−General's Department, Australian Federal Police and other police forces).
3. *Telecommunications Interception Legislation Amendment Bill 2002*
    - ♦ Report of the Senate Legal and Constitutional Legislation Committee, 8 May 2002

About EFA

Electronic Frontiers Australia Inc. ("EFA") is a non−profit national organisation representing Internet users concerned with on−line rights and freedoms. EFA was established in January 1994 and incorporated under the *Associations Incorporation Act* (S.A.) in May 1994.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of users of computer based communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of computer based communications systems.

EFA policy formulation, decision making and oversight of organisational activities are the responsibility of the EFA Board of Management. The ten elected Board Members act in a voluntary capacity; they are not remunerated for time spent on EFA activities. The role of Executive Director was established in 1999 and reports to the Board.

EFA has long been an advocate for the privacy rights of users of the Internet and other telecommunications and computer based communication systems. EFA's Executive Director was an invited member of the Federal Privacy Commissioner's National Privacy Principles Guidelines Reference Group and Research Reference Committee during 2001. EFA participated in NOIE's privacy impact assessment consultative group relating to the development of a Commonwealth Government Authentication Framework in 2003 and is currently participating in the ENUM Privacy and Security Working Group convened by the Australian Communications Authority. EFA has presented oral testimony to Federal Parliamentary Committee inquiries into privacy related matters, including amendments to the Privacy Act 1988 to cover the private sector, telecommunications interception laws, cybercrime, spam, etc.