Submission of the

NEW SOUTH WALES COUNCIL FOR CIVIL LIBERTIES

to the

Senate Legal and Constitutional Committee's

Inquiry into the Provisions of the

Telecommunications (Interception) Amendment Bill 2006

13 March 2006

Author: Dr Martin Bibby

Introduction

The Council thanks the Committee for the invitation to comment on this Bill.

It should be noted from the start that this Bill is not about terrorism.

The issue with this bill is whether privacy means anything at all in Australia. It is proposed to allow a slew of organisations to have access to emails and SMS messages—what are called stored communications. It is proposed to do this where there is no threat to life or limb, and no major corruption to weed out. For this kind of surveillance, it is proposed to introduce lower reporting requirements than those that that apply to interception of voice transmissions. It is proposed to increase the classes of authorities who can be approached to issue warrants.

No argument is given in the Explanatory Memorandum or in any of the second reading speeches to support these proposals[1].

Even worse, is the intention to legalise the bugging of telephones of third parties—of people who are not suspected of complicity in the planning of crimes, but who are **thought** to be in contact with the person who is **thought** may be a criminal. The conversations of the so-called B-party, and those of his or her spouse, and of their children, may all be listened to, recorded, transcribed, and copies made.

It is conceded that legislation is needed to clear up the mess concerning access to stored communications. But this bill clears up the mess by throwing away the china. Surveillance of stored communications should be subject to the same restrictions as interception of live conversations; the reasons that support the latter apply equally to the former.

The bill is not all bad. There is a new requirement for the courts to take into account the effects upon privacy before permission is given for surveillance that is connected with what at present are classified as class one crimes—the more serious crimes. There is an effort made to limit the possibilities of abuse. People whose privacy is violated by illegal access to stored communications are to be able to seek remedies under both the civil and criminal law—as they can at present after illegal interception of live telecommunications. Similarly, a court must take into account whether the agency which seeks a warrant has other means of obtaining evidence. We believe the requirement should be more strict, both for stored communication warrants and for interception warrants.

[1] The nearest to an argument is a question-begging comment that the requirements for access to stored communications lie between the requirements for search warrants and those for interception of spoken communications. But the issue is, precisely, whether there is any reason why they should be in the middle; why the requirements should be any less than those for interception.

Summary of Recommendations

Recommendation 1: That an issuing authority for stored communication warrants should be prohibited from issuing one unless the applicant agency has exhausted all other practicable methods or investigation.
Further, that an issuing authority for interception warrants should be similarly restricted.

Recommendation 2: That the same threshold that applies to interception of conversations should apply also to stored communications.

Recommendation 3: That only the agencies that are permitted to apply for interception warrants be permitted to apply for stored communications warrants.

Recommendation 4: That only judges be authorised to issue warrants under the Telecommunications (Interception) Act.

Recommendation 5: That the reporting requirements for stored communication warrants be as rigorous as those for interception warrants.

Recommendation 6: That evidence obtained in investigating one offence be not usable in proceedings in relation to contraventions which carry a penalty of less than 7 years' imprisonment.

Recommendation 7: That the proposal for B-party interception be deleted from the Bill.

Recommendation 8: That if Schedule 2 (B-party Interception) is to proceed, the threshold for the issue of warrants be warranted belief that there is an imminent threat to life.

Recommendation 9: That the CEO of each agency that acts upon a telecommunications warrant be required, no more than two years later, to inform the target of the fact that interceptions and/or access to stored communications have taken place, and when this occurred, subject to the following conditions.

i. The CEO may determine that release of the information would jeopardize an ongoing investigation. This power should not be delegable.
ii. Where the power proposed in sub-recommendation i. is exercised, a report must be made to the Ombudsman or the Director General of Security and Intelligence as appropriate.
iii. The decision that the information about warrants is to be withheld should be challengeable in the courts.
iv. Where a decision has been made not to release information about action taken on a warrant, the information must be released, subject to the same conditions, within a further two years.

Recommendation 10: That if B-party warrants are instituted, the CEO of each agency be required also to inform the B-party that interceptions and/or access have taken place, subject to the same conditions.

Recommendation 11: That if Schedule 2 (B-party warrants) is to proceed, then it be amended to permit only judges to issue B-party warrants.

Recommendation 12: That if Schedule 2 (B-party warrants) is to proceed, then evidence obtained with the use of such warrants be not usable in proceedings other than those involving the killing of persons or threats of such killing.

Recommendation 13: That the Committee resist any attempts to give powers to make decisions that permanently or for significant periods affect the fundamental rights of any individual (including the rights to liberty, citizenship, residency, fair trial, freedom of expression, thought conscience and religion and voting entitlement) unless those decisions can be challenged effectively in the courts. Organisations that obtain information covertly should not be given such powers at all.

1. Stored Communications

It is desirable that the law concerning the accessing of stored communications should be clarified. The Council for Civil Liberties (CCL) appreciates that in seeking to do so, efforts have been made to ensure that the contents of those communications are not made known outside the group of institutions that it is intended will collect them.

It is appreciated also that with the dropping of the distinction between Class One and Class Two offences, an authority who issues a telecommunications warrant will have to weigh the severity of the invasion of privacy against the gravity of the offence in all cases.

However, the regime proposed for stored communications is inferior to that which exists for interceptions in several respects. No good reason has been offered for these differences.

The reasons for restricting access to stored communications are the same as those for restricting interceptions.

The most common varieties of stored communications are emails that have not yet been accessed by the intended recipient, unexamined SMS messages and voicemail or phonebank messages.

All of them are used to have conversations. The content can be as trivial or as profoundly personal as a live conversation. They can be conversations between a parent and a child in trouble; between a counsellor in an agency and a person who is contemplating suicide; contain medical details; involve messages of love and affection. They can contain scraps of information which, looked at out of context, will be misleading. They may contain criticisms of persons which will cause great damage if made public.

These interactions will be inhibited or made practically impossible if it becomes known that there are snoopers “listening” to these conversations.

All the other reasons that there are for protecting the privacy of telephone conversations also apply to the privacy of stored communications. There is no relevant difference that justifies different treatment. No such difference has been presented in the Explanatory Memorandum, nor in any of the second reading speeches.

1.1 Alternatives to access and interception

The proposals in the Bill concerning stored communications suppose that it does not really matter if privacy is invaded, provided it is the police, ASIO or other enforcement agencies that are doing the snooping. It cannot be emphasized enough that eavesdropping, interception, or accessing private communications are wrongs. They are wrong whether they are done by

private individuals, by anti-corruption bodies, by police or by ASIO. They cannot be justified merely because they are useful.

Because they are wrong, their use should be limited. They must never be a substitute for ordinary policing. It should not be enough to say that they 'would be likely to assist in connection with the investigation by the agency of a serious contravention in which the person is involved'.[2] The circumstances must be that the applicant agency **cannot reasonably use** other methods to obtain the information it needs.

An issuing authority is to be required to have regard to:

> (d) to what extent methods of investigating the serious contravention that do not involve the use of a stored communications warrant in relation to the person have been used by, or are available to, the agency; and
> (e) how much the use of such methods would be likely to assist in connection with the investigation by the agency of the serious contravention; and
> (f) how much the use of such methods would be likely to prejudice the investigation by the agency of the serious contravention, whether because of delay or for any other reason.[3]

It is submitted that, rather than merely having regard to these matters, an issuing authority should prohibited from issuing a warrant if such methods are available. A wording similar to that found in item 3 of Schedule 2 could be used: the issuing authority should be prohibited from issuing a warrant unless the agency has exhausted all other practicable methods or investigation.

This change would also deal with a further problem. The proposed powers would enable an agency to access financial records such as bank records, and superannuation statements, in order to investigate tax offenses or other financial contraventions—and to do so covertly. It could access medical records while investigating fraud. At present such records are accessible by the use of search warrants, which are overt and can be challenged. They define what may be obtained, the time of day when the warrant may be executed, and they prevent fishing expeditions. Thus privacy is protected except in those cases where it can be shown to be justifiable to invade it. That should apply here also.

[2] Proposed subsection 116(1)(d).
[3] Proposed subsection 116(2).

Recommendation 1: That an issuing authority for stored communication warrants should be prohibited from issuing one unless the applicant agency has exhausted all other practicable methods or investigation.

Further, that an issuing authority for interception warrants should be similarly restricted.

1.2 The threshold

Under item 2 of Schedule 1[4], contraventions of the law with a maximum penalty of three years' imprisonment or 180 penalty units are to be serious contraventions. A person who is suspected of having committed such a contravention may have their stored communications examined.

By comparison, interception of conversations is only permitted if the law that has been contravened is punishable by seven years' imprisonment.

The person need have committed no crime at all. All that is required is a reasonable suspicion that they might be going to commit a crime. (One must assume that the investigating agency does not have good evidence of conspiracy to commit a crime, since conspiracy is a crime itself and there would be no need for the surveillance.)

As is argued on page two above, the invasion of privacy involved in accessing emails is no less than that in intercepting live conversations.

Accessing emails is not like executing a search warrant. As was noted above, the existence of a search warrant and the actions taken in accordance with it are generally overt; and this gives the person against whom it is issued opportunities to challenge the warrant and the actions, and to defend themselves against false inferences that are drawn from what is discovered. But accessing stored communications is covert. It would lose most if its purposes if it were not. Accordingly the person is defenseless against the invasion of privacy. The tougher standard that applies to interception of conversations should apply.

Recommendation 2: That the same threshold that applies to interception of conversations should apply also to stored communications.

1.3 The variety of agencies permitted to apply for warrants

The Bill proposes that a wider range of agencies should be permitted to access stored communications. This increase is given no separate justification. We presume it relates to the lesser threshold: more agencies are involved because the contraventions of more laws are included. If this is

[4] Proposed section 5E.

the case, then arguments against lowering the threshold are also arguments against broadening the range of agencies.

Further, every increase in the authorities authorized to access private communications increases the likelihood of abuse, and of private information being made public. Senate Committee members may be aware of a recent case [5] in which a well-respected solicitor who has been given a security clearance was nevertheless denied access to evidence important to his client's case on the grounds that he might *inadvertently* release the information. If such a man might make slips, the same must apply to members of the agencies that it is intended be included. The wider the group of people who have access to emails and SMS messages, the higher the risk of inadvertent disclosure.

The larger the group of agencies, moreover, the more difficult it will be for proper supervision to take place.

Recommendation 3: That only the agencies that are permitted to apply for interception warrants be permitted to apply for stored communications warrants.

1.4 The increase in issuing authorities.

There is no explanation for the increase proposed in issuing authorities. It may relate to the increase that is proposed in agencies permitted to seek warrants (and so, indirectly, to the reduction of the threshold). It must relate to an expected increase in applications, and perhaps in warrants.

If the above arguments are accepted, there should be no increase in warrants. Australia has already seen a steep increase in the number of warrants issued for this kind of purpose. It is reasonable to ask why. If warrants are less effective than they were, there should be fewer requests for them, not more.

There is reason to believe that warrants are issued too readily.

Applications for warrants (for the years to June) have been: (1996-7) 638, (1997-8) 684, (1998-9) 1286. (1999-2000) 1696, (2000-01) 2164) (2001-2) 2518, (2002-3) 3067, (2003-4) 3059.

31 requests were rejected or withdrawn in the last year. In the other years, the average was only 7.[6] Assuming that some of those were withdrawn rather than rejected, it is hard to escape the conclusion that the issuing authorities are not doing their job properly.

[5] *Traljesic v Attorney-General of the Commonwealth of Australia* [2006] FCA 125 (9 February 2006).

[6] Source: Attorney General's annual reports to Parliament.

We have argued previously[7] that

> 'The number of warrants issued annually in Australia under the Telecommunications (Interception) Act (the TIA) has been increasing substantially, to the point where it exceeds the number issued for similar purposes in the United States of America. There are few refusals of requests for warrants, and none from any member of the Administrative Appeals Tribunal. There has been no significant increase in the number of such crimes reported, to justify this increase. Nor has there been a commensurate increase in criminal convictions of the most serious crimes.'

In his second reading speech, the Attorney General questioned the significance of this comparison, asserting that the US figures do not include those interceptions that are considered sensitive on security grounds.

But the Australian figures also do not include ASIO warrants. The figures are reasonably comparable. Yet the risk to the United States from terrorists and from organised crime is far higher than it is in Australia.[8]

It is also striking that in 2003-4, 2302 of the warrants were issued by members of the Administrative Appeals Tribunal. 494 were issued by Federal Magistrates, 179 by Family Court Judges, and only 53 by Federal Court Judges. It is tempting to draw the conclusion that AAT members are a soft touch—or to put the matter more precisely, that they are not properly concerned to balance the privacy of targets and their families against the desire of enforcement agencies for quick convictions. And that is why the overwhelming majority of applications are made to them.

This conclusion is supported by the trial data. In 2002-2003, material was used in securing only 1225 convictions, and in 2003-2004, 1824.

Recommendation 4: That only judges be authorised to issue warrants under the Telecommunications (Interception) Act.

1.5 Lower reporting requirements

Consistently with the arguments above, agencies (including ASIO), the Ombudsman, the Inspector General of Intelligence and Security and the Minister should have to report as extensively as is required for interception of conversations.

[7] Submission to the Senate Legal and Constitutional Committee, The Crimes Legislation Amendment (Telecommunications Interception and Other Measures) Bill 2005, page 1.
[8] A comparison was also made with Germany. But the German figures include **all** interceptions.

Recommendation 5: That the reporting requirements for stored communication warrants be as rigorous as those for interception warrants.

1.6 Flow on uses

The Bill would allow information obtained from accessing stored communications to be used in proceedings where the penalty is only one year's imprisonment; and once the material has been used in a trial, for it to be able to be used in any proceeding at all.

This possibility is an inducement to police and other authorities to go on fishing expeditions—to seek a warrant for an offence carrying a penalty of 3 (or 7) years' imprisonment, and then to use the entitlement thus gained to hunt for evidence about other offences. Thus the principal intention of the Act, to protect privacy, will be subverted.

It is one thing to argue that if it is found that a life is at stake, or that a murder has taken place, that it would be irresponsible not to act to protect a potential victim. The case is quite different with the lesser offences contemplated by the Bill.

The best way of avoiding this is to confine the use of material obtained pursuant to a warrant to the investigation of contraventions that would themselves provide the grounds for the issue of a fresh warrant.

Recommendation 6: That evidence obtained in investigating one offence be not usable in proceedings in relation to contraventions which carry a penalty of less than 7 years' imprisonment.

2. B-party warrants

The proposal in schedule 2 of the Bill for B-party warrants involves a major intrusion on the privacy of innocent persons—perhaps the greatest that has been proposed since the Federal Parliament began.

It is intended that ASIO will be able to intercept the telephone calls and other communications of innocent persons, about whom there is not a shred of suspicion, in the hope of obtaining information about another person. There is no restriction on who the B-party will be. It could be a spouse, a child, the lawyer, a clergyman—whoever is handiest, or whoever the agency has knowledge of. All their conversations may be monitored, not just those with the suspected transgressor.

The proposal is contrary to Article 17 of the *United Nations International Covenant on Civil and Political Rights*, to which Australia is a signatory, which reads:

> 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.

The proposal should be rejected.

It is argued that B-party interception is necessary because criminals are becoming more knowledgeable about ways of avoiding surveillance, changing SIM cards frequently, for example, and changing the telephones that they use. The law is to be changed to keep up with them.

The trouble with this argument is that there is no end to the process. It will only take a bit of ingenuity to find ways of avoiding the newly permitted surveillance. What will happen then? As criminals get to be more cunning in finding ways to avoid surveillance, so the case will be made for more and more intrusions into privacy. Yet that will not solve the problem. Unless privacy is to mean nothing when a law enforcement agency wants to invade it, a limit must be set. It is the CCL's contention that this proposal goes over the limit.

Further, what the argument presupposes is that interception is no longer a great solver of crimes. As the Attorney General himself puts it 'I would like to think that telecommunications interception could be as effective as it has been in the past, but the concern we have is that, as a useful tool, it is being significantly degraded.'[9]

[9] Speech in reply to the second reading debate, Hansard 01 March 2006, p. 8 (9.45 a.m.).

We should not, then, be throwing more and more of our privacy away, like a First World War general throwing more and more troops into fruitless battle.

Further, there is a problem of what might be called synergism. It proposed[10] to give ASIO the power to reject applications for citizenship, without the option for ministerial discretion, and, as is becoming usual, without the applicant being given any reasons. There is talk of an Australian identity card, with links to electronic databases. There are now powers to detain people or to subject them to severe restrictions on their liberty on the basis of mere suspicion. The power proposed in Schedule 2 will make it more likely that those other powers are misused, since there will be more opportunity for innocent remarks to be misconstrued, and unrelated comments to be put together, with false inferences being drawn.[11]

Recommendation 7: That the proposal for B-party interception be deleted from the Bill.

[10] In the Australian Citizenship Bill 2005.

[11] There are, as members would be aware, standard arguments about privacy.

3. Safeguards

If, in spite of these arguments, this part of the Bill is to proceed, then it is vital that additional safeguards are put in place.

3.1 Raising the threshold

Since the motivation in putting forward this part of the Bill is the desire to protect human life, the entitlement to issue warrants should be limited to cases where there is imminent threat to life.

The threshold therefore should not refer to penalties, since there are draconian penalties in place for such things as threatening to disrupt a transport system.

Recommendation 8: That if Schedule 2 (B-party Interception) is to proceed, the threshold for the issue of warrants be warranted belief that there is an imminent threat to life.

3.2 Release of warrant information

Two years after a B-party warrant is acted upon, the information that interception took place, and when it took place, should normally be released to the B-party. Two years after any telecommunications warrant is acted on, the same information should be released to the target.

This would bring several benefits. It would enable a person who has been harmed by an improper interception to seek redress. It would enable innocent targets to clear themselves of the suspicion that led to their being spied upon in the first place. People who believed, but could not prove, that the police or ASIO agents had acted wrongly would be able to ask for the Ombudsman or the Director General of Security and Intelligence for an investigation. The threat of adverse findings might well make agents and police wary of misuse of their powers.

There are some obvious difficulties, so the precise arrangements for this need some care. There would need to be a safeguard against the release of information that is still sensitive—where an investigation is continuing, for instance, and there are good reasons for it to have taken so long. CCL suggests that the heads of the relevant agencies should be given power to delay the release, with reasons. That decision in its turn should be challengeable, lest it be used capriciously or to hide mistakes or deliberate misuse of the powers that are being poured on police. Each decision to deny or delay release should lead to an automatic investigation by the Ombudsman or the Inspector General of Security and Intelligence.

Recommendation 9. That the CEO of each agency that acts upon a telecommunications warrant be required, no more than two years later, to inform the target of the fact that interceptions and/or access to stored communications have taken place, and when this occurred, subject to the following conditions:

i. The CEO may determine that release of the information would jeopardize an ongoing investigation. This power should not be delegable.

ii. Where the power proposed in sub-recommendation i. is exercised, a report must be made to the Ombudsman or the Director General of Security and Intelligence as appropriate.

iii. The decision that the information about warrants is to be withheld should be challengeable in the courts.

iv. Where a decision has been made not to release information about action taken on a warrant, the information must be released, subject to the same conditions, within a further two years.

Recommendation 10. That if B-party warrants are instituted, the CEO of each agency be required also to inform the B-party that interceptions and/or access have taken place, subject to the same conditions.

3.3 Issuing Authorities and flow on

If recommendation 4 above is not accepted, the restriction to judges should at least apply to B-party warrants.

Similarly, there should be no use of information gathered by this extraordinary means in dealing with lesser crimes. The use of information in proceedings dealing with other crimes should be limited to cases where life has been threatened or taken.

Recommendation 11: That if Schedule 2 (B-party warrants) is to proceed, then it be amended to permit only judges to issue B-party warrants.

Recommendation 12: That if Schedule 2 (B-party warrants) is to proceed, then evidence obtained with the use of such warrants be not usable in proceedings other than those involving the killing of persons or threats of such killing.

3.4 The problem of synergism

As was argued above,[12] a synergism can occur when powers to obtain information covertly are combined with powers to make decisions that affect individuals' exercise of their rights. There is too much risk that innocent remarks will be misconstrued and be combined with unrelated comments, with false inferences being drawn.

ASIO, the AFP and the other organisations that will have access to intercepted materials must not be given unchallengeable powers to determine whether people are free, or whether they are allowed to stay in the country, or whether they are allowed to become citizens. Nor should any Minister have such unchallengeable powers.

In the present context, it is almost unbearable to think that ASIO might become incompetent. We have to remember that however competent it may be at present, it was by no means so in the past. In the 1970's, its then Director-General declared its first loyalty lay to "the West". That, he said, was more important than democracy and more important than the integrity of Australian institutions. At the same time, extravagant conclusions were drawn from the flimsiest of evidence about the dangers that members of parliament, trade union officials, academics, and anybody who challenged ASIO's actions, posed to "the West". Ordinary democratic activities were treated as highly suspect. Those who demanded ASIO's reform were called cowboys.

In the next decade, the Federal Parliament itself joined the cowboys, after the nonsense about agents of influence, and created the office of Director General of Security and Intelligence, while increasing parliamentary oversight. The period of ASIO's incompetence is now known as 'ASIO's cowboy days'.

Though there are now some safeguards, incompetence can return. ASIO in particular is susceptible to this, since its functions require it to be suspicious where there is very little ground for suspicion. Precisely because the present times are so dangerous, its susceptibility is increased.

We have to remember also that although there have been efforts to remove corruption for the Federal Police, corruption has been suspected and action taken to deal with it relatively recently. State Police forces have notoriously been both corrupt and incompetent, with problems reaching commissioner level.

Thus the risk that "information" gleaned from intercepts will be misinterpreted, combined with other material to draw mistaken conclusions and then applied inappropriately is no mere theoretical possibility. No decisions that limit the exercise of fundamental rights should be taken without those affected having access to a fair hearing.

[12] In section 2.

Recommendation 13. That the Committee resist any attempts to give powers to make decisions that permanently or for significant periods affect the fundamental rights of any individual (including the rights to liberty, citizenship, residency, fair trial, freedom of expression, thought conscience and religion and voting entitlement) unless those decisions can be challenged effectively in the courts. Organisations that obtain information covertly should not be given such powers at all.