Duncan Kerr SC MP

Federal Member for Denison

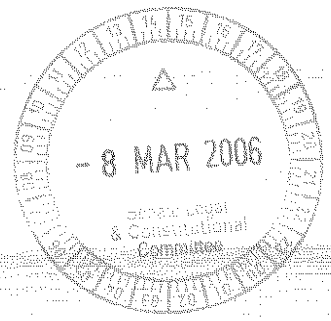
188 Collins St, Hobart 7000

Ph (03) 6234 5255 Fax (03) 6223 8560

GPO Box 32 Hobart Tas. 7001

6 March 2006

Jonathan Curtis
Committee Secretary
Senate Legal and Constitutional Committee
Department of the Senate
Parliament House
Canberra ACT 2600



Dear Jonathan

Please find attached remarks on the *Telecommunications (Interception) Amendment Bill 2006* as a submission to the enquiry held by the Legal and Constitutional Committee in relation to this bill.

Yours sincerely

Duncan Kerr SC MP
Federal member for Denison

Parliament House Canberra ACT 2600

Telephone (02) 6277 2178

TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT BILL 2006

Second Reading

Mr KERR (Denison) (8.32 p.m.)—There are significant elements of the Telecommunications (Interception) Amendment Bill 2006 to be welcomed, but I think it is important for me to set out some of the concerns I have and am certain are shared more broadly throughout many sectors of the community and on both sides of this House with respect to the detail. There is no doubt that the motivation for this legislation is well based and many of the initiatives will clarify the entitlement of law enforcement to secure information that is required for proper law enforcement purposes. In making those circumstances transparent and setting out clearly the manner in which interceptions can be undertaken in respect of a number of areas which presently lack sufficient clarity, the intention of the minister, the government and the opposition, in indicating its support for the general approach, is to be welcomed. But I do want to draw attention to some of the areas which require the further consideration of this parliament. I note that this legislation will be subject to further review by the Senate Legal and Constitutional Legislation Committee, and the remarks I make now are in the context that I hope the issues I raise are taken into account by those participating, and I intend to forward the text of these remarks to that committee to be taken into account as a submission in their deliberations.

The first issue I want to turn to by way of expressing concern goes to the question of stored communications. It is certainly true that one of the issues that has confronted law enforcement is how to effectively deal with communications which are carried in an electronic form that are not the traditional voice messages carried over phone lines. The telecommunications interception regime that was put in place in 1979 envisaged handsets connected by copper wire hardlines and set out a regime at first limited to a very narrow range of offences and available only to Commonwealth law enforcement agencies but subsequently extended to a much wider range of offences and permitted to be utilised by state and territory law enforcement agencies and a range of commissions charged with the responsibility for anti-corruption matters.

These extensions have each been deliberated upon and considered, but one of the technological innovations that has occurred of course is the growing use of electronic transmissions to carry not only voice messages but also text messages and stored communications. We all use mobile phones whereby we receive text messages transmitted to us by friends, colleagues and acquaintances. We often use hand-held devices—BlackBerries and the like—to communicate not only short messages but also messages which include attachments and to file and store large amounts of documentation.

My concern is that we are not putting in place the same strict regime for accessing this so-called stored communication as we do for regulating the interception of telecommunications that are voice messages over hardlines. The tests we have enacted to permit access to interception of voice transmissions remain very high. The regime is not one which, in my view, is capable of being easily subverted by those who would be frivolous about seeking to utilise such interception methods. But the proposed test in respect of stored communications is much lesser. I am troubled by the reasoning behind the proposition that my privacy is much less intruded upon if the message I receive on my mobile phone or a message that is transferred through a BlackBerry and an email attachment is intercepted covertly, unknown to me. Why should the test be lesser in those circumstances than it would be for an interception of a voice transmission?

I think the argument is put that a lesser test is appropriate because it is more in the nature of a search warrant that could be issued under the various search warrants legislation for hard copy material—that is, the test ought be more analogous to the kind of test that would apply were, for example, a search to be authorised of a person's office or home for materials that were suspected of being evidence in relation to a possible crime. The problem with that analogy is that, in the large majority of—almost all—instances where search warrants are pursued, the person against whom the search warrant is issued comes to learn of its issue and can contest the issue of the warrant on the basis that it was issued improperly. In relation to the materials that have been the subject of seizure, they can make claims of legal professional privilege or, in the instance of members of parliament, parliamentary privilege. There is a range of other circumstances in which people can raise properly those objections to an overwide use of those powers.

But, in the case of the interception of stored communications, it is much in the nature of a telephone interception: you do not come to know of it. So it is a covert interception. As we move more and more of our business from paper based to electronic storage of information, what we are effectively doing is permitting, at a much lower test, covert interception of large amounts of stored materials. It is a test which is not examinable in the same way as ordinary search warrants are and with a lesser threshold to meet than we insist upon with voice communication. I think this is quite troubling and I suggest that the Senate have a look at this. Two possible solutions commend themselves. One would be to have the same high-level test for the seizures of covertly obtained materials where a warrant for stored communications is sought; the other would be to require, where the lesser test applies, the person to be notified of the collection as one would normally find out about the implementation of the search warrant so that the ordinary claims for privilege and the various other entitlements to challenge the issue of the warrant, the legality of it and the grounds for it can be pursued.

It seems to me that we are introducing effectively a much more comprehensive regime to permit access to substantial amounts of electronically stored material, which is now the most common form of commerce, in a way which does not give the traditional safeguards to those against whom the decision was made. I might say in respect of one matter of most moment to members of this parliament that it would bypass the arrangements that have been entered into between the Speaker and the President of the Senate and the Australian Federal Police regarding seizures of materials relating to parliamentarians' conduct of their business in this House. Presently, there is an arrangement in relation to the exercise of a search warrant which enables members to make properly founded claims for privilege, to have those claims examined and to have the warrant dealt with in a manner which accommodates those entitlements. That, of course, could not occur if the member does not know that they have been the subject of an interception. And, in a like manner, the entitlements the ordinary citizen has to make claims of legal professional privilege or to challenge the evidential and legal basis for the issue of a warrant, to claim that it has been issued in circumstances where it is impermissible to issue it, is not available simply because they do not know that the seizure has occurred. I put these arguments forward on the basis of long experience as to how these matters do operate, having served myself for three years as Minister for Justice responsible for the Australian Federal Police in this parliament and previously having had responsibility for arguing a number of cases before superior courts about the validity of warrants issued in relation to searches and seizures.

The second point that I turn to is a point that has been given a greater degree of attention than that which I have just discussed, and that is the so-called B-party warrants. These are extremely contentious because, for the first time, our law will permit an issuing authority to authorise the interception not of the phone service used by a person against whom a suspicion is held but of any innocent third party against whom no such grounds are established in order that they might incidentally collect through that means the communications of the person against whom the suspicion is held. I have given earnest thought to the justification for this, and reluctantly I accept that there is a proper basis for permitting the use of B-party warrants but would like to see far greater safeguards than are presently encompassed in the legislation. Why have I conceded that it may be legitimate to use B-party warrants? I might say that the euphemism of a B-party warrant is something that I find little offensive. They should be called 'innocent third party warrants' or 'third party warrants' because I think that by the use of such language we really do not come to the gravamen of the point. But it is a truth that, as we have gone now over 25 years since first authorising telephonic interception, not only has law enforcement come to rely on them and use them more effectively but so too have those against whom they are sought and directed become somewhat smarter in their capacity to hide their communications from the authorities.

I do not think it is giving away any great law enforcement secrets to mention the fact that there are people out there, 'smarties', who are trying to switch hand-services and chips on a regular basis so that it is difficult to find out what service they are using and to follow and trace the calls they are making. If that is a practical problem in tracing and identifying the telecommunications of persons against whom warrants would lawfully be issued, I think it is reasonable for this parliament to say, 'In those circumstances we will permit the collection. If we can't get at this through ordinary means, we will permit law enforcement to seek authority to tap the phones, to intercept the communications, of persons we believe they are in communication with—third parties.' It may be lawyers, it may be accountants, it may be family, it may be friends, it may be people with whom they have business relations of an innocent kind or it may be parliamentarians whose constituents are suspected of particular conduct, and in this means by tracing these innocent third parties, intercepting the calls of the innocent third parties, find out what the target is seeking to do, identify the phone services they are using, where they reside, what they are doing and follow their conduct, and, hopefully, obtain evidence that may be material to either preventing crime or prosecuting it.

The problem I see, however, is that there is a very grave risk that, in permitting this, we are going to open up a whole range of collateral material to intrusion, investigation and collection that we do not intend to bring into the net. It seems to me that if the government's purpose is not to expand the right of law enforcement to seek warrants against innocent third parties per se so that their communications are not only with the suspected wrongdoer but with other parties—let us assume party A is a suspected wrongdoer and party B is known to have some contact with that person but against whom there is no suspicion of wrongdoing; you could not normally issue a warrant against party B—this legislation will now permit that but will bring into the net all the communications between parties B, C, D, E and F and all the people they call.

If the real intent of this legislation is to collect material that is being evaded because party A is using sophisticated means to prevent the detection of their communications, let us allow that but make certain that we quarantine the communications to those which would have been lawful under the previous

interception regime had it been possible to collect the material by direct interception of party A. Let us not open up the possibility of innocent third parties being now roped into a very much expanded net of telecommunications which we have never intended in this parliament to open up.

If it is the government's intention simply to make certain that evasion is not possible through the means that are currently being adopted, we should quarantine third party communications so that the subsequent communications between parties B, C, D, E and F must not be collected, must not be held, and that material that might otherwise be available were it collected is made subject to both use and indemnity use privilege so that it cannot be used as evidence. If we are seeking to make certain our regime is effective so that it cannot be avoided, we should not be opening up a regime that exposes a whole range of additional people against whom law enforcement has no proper basis for seeking warrants to the whole of their communications with a whole range of other people which would not have been available to the law enforcement agency previously in such a way.

So I think the onus is on the government to tell us why, if they are not prepared to accept that proposition, they want to be able to use this further material far beyond that which they have asserted is the reason for this B-party regime. If the B-party regime is intended to allow the collection against party A, and that is all the communication between A and B—that is, communication that would have been capable of collection if party A had not avoided the warrant—it should not be a basis for extending the regime against parties whose communications would not be the subject of warrant because, under the law as it stands, there would be no proper basis for its collection. We should not be opening this up further.

This is not an issue of addressing a problem that currently is a common-law issue. That is a nonsense argument that has been put forward. The only lawful basis for the interception of a telephone service in Australia now is under the Telecommunications (Interception) Act. There is no basis whatsoever to suggest that there is a common-law right for third party, B-party, interceptions. That is an absolutely absurd red herring that has been thrown into this debate—I do not understand on what legal basis or proposition—by members on the other side. It is a nonsense.

With those remarks, I accept that we do need to clarify the way in which we address some of these issues, but I do not think that the safeguards that have been put in place are consistent with the understanding that the government has advanced for the rationale and the protection of the broader community interests that are also as important as making certain that law enforcement cannot be avoided. I accept, as somebody has had the responsibility, that high levels of government and law enforcement must be made efficient and effective, but I also believe that this parliament has a high responsibility for protecting individual rights. *(Time expired)*