



**TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT BILL  
2006  
Second Reading  
1 March 2006**

[Ms GRIERSON](#) (Newcastle) (9.17 a.m.)—I rise today to speak on the [Telecommunications \(Interception\) Amendment Bill 2006](#). The intent of this legislation is to amend the Telecommunications (Interception) Act 1979 to implement certain recommendations of the Blunn report on the regulation of access to communications under the act.

Clearly, the world is changing rapidly, and the way we communicate with each other has evolved from telegraph, fixed telephone and postal delivery to mobile phone, text messages, emails and digital communications in a very short space of time. These changes have brought with them huge benefits to individuals and to our community in efficiency, convenience and productivity. But they also bring new opportunities for those who seek to plan and carry out crime. People who would commit crime can use this new technology to improve their own efficiency, convenience and illicit productivity. The changes in communications technology have clearly brought with them changes in the ways in which people use those technologies for criminal purposes. It stands to reason, then, that the way in which our law enforcement agencies approach the prevention and investigation of crime must also change.

I am pleased to see that the government has responded to the recommendations of the *Report of the review of the regulation of access to communications*—known as the Blunn report. Labor pushed strongly for an independent review of access to communications by enforcement agencies. I am particularly pleased to note Mr Blunn's first finding:

... the protection of privacy should continue to be a fundamental consideration in, and the starting point for, any legislation providing access to telecommunications for security and law enforcement purposes ...

I firmly believe that all of us, as legislators, should bear those words in mind as we consider this legislation. No matter how quickly telecommunications and technologies change, and how quickly criminals change their behaviour to take advantage of this, there is one thing that never changes—the right of every Australian citizen to have their privacy and civil liberties protected.

The right to privacy is fundamental, and we must not let our quest to prevent crime impinge upon this right. No matter how quickly the world

changes, there are some fundamental rights which must always be defended. That is why I have to say that I have mixed feelings on this legislation. The legislation is an attempt to clarify the powers of law enforcement and security agencies to access both real-time communications and stored communications—and, of course, stored communications now are very extensive. It is only sensible to do this. But I do have concerns about the implications of this legislation. I am glad to see that it has been referred to a Senate committee for closer scrutiny, and I hope that any unintended consequences are revealed and removed from the legislation in that process.

It is vitally important that we get legislation such as this right. We have seen this government rush many pieces of controversial legislation through this place and through the Senate without proper scrutiny or investigation. I fear that legislation such as the Work Choices bill, the Welfare to Work bill and the sedition provisions of the antiterrorist legislation will have implications as they progress and are implemented. Those implications will be felt by our communities. It is, then, important that this legislation is scrutinised fully in the Senate committee process. The key, as we have so often seen in our post September 11 world, is to strike a balance—a balance between our desire to protect the civil liberties of our people and our desire to keep our people safe.

There are several key provisions in this legislation to enact certain recommendations of the Blunn review. They deserve examination. Firstly, the legislation inserts a warrant regime for access to stored communications held by a telecommunications carrier. These stored communications are broadly defined to include electronic messages located on a computer, internet server or other equipment, whether read or unread, opened or unopened—messages such as emails, text messages, voice mail and all the attachments. Such stored communications are presently not covered by the Telecommunications Act, so they could be intercepted within the existing warrant regime without the need for a telecommunications interception warrant. However, this existing warrant regime has limitations and offers fewer protections than a telecommunications interception warrant should.

The legislation before us does propose a new warrants regime that will move stored communications from a general search warrant to tougher provisions similar to those already in the Telecommunications (Interception) Act for real-time communications. On balance, this appears to be a sensible amendment which recognises the change in telecommunications methods since the original interception act was drafted.

Schedule 3 of this legislation sets out to amend the named telecommunications interception warrant provisions to enable agencies to intercept communications to and from identified devices such as mobile phone handsets, personal and laptop computers, personal digital assistants and pagers. I note that interception on the basis of the device must only be authorised where the applicant agency has no practical method of identifying

the telecommunications service used or likely to be used by the person of interest and that the interception of those services would not be possible.

Again, this provision appears to be necessary to keep up with the changing nature of communications and the way in which suspected criminals can use a large number of devices and services to disguise their activities. That can involve changing email services or mobile phone SIM cards to make it very difficult to track and link communications to the person of interest. As such, the provisions to allow for interception warrants to be issued in relation to specific telecommunications equipment appear to be useful ones.

The other major schedule in this legislation that I wish to discuss today is the schedule dealing with so-called B-party intercepts or third-party intercepts. Like the equipment based interception provisions that I referred to, this schedule has been introduced in an attempt to allow another way for enforcement agencies to intercept the communications of people of interest when they are having difficulty doing so through the usual channels of an interception warrant.

However, the problem many Australians would have with this schedule is that it does not only target people who are suspected of a crime or the equipment and services they use. B-party intercepts allow persons other than the person suspected of involvement in the crime to have their communications intercepted. These persons are referred to as the B-party. As long as this B-party is in contact with a suspected person, no matter what they are talking about or what information they are exchanging, that B-party person can then have their communications intercepted. Let us be clear what this means: a warrant can be obtained to bug the phone of a person who is not suspected of a crime. We should think very hard about the implications of this and the safeguards that are required before proceeding.

If party A, the person under investigation, is having their communications intercepted and they are discussing proposed crime with party B, then I have no problem with party B being brought into the scope of that investigation. What I do have a problem with is what the implications are of a B-party interception warrant then being issued for the second party. And, of course, that is the sort of safeguard that I would like to see.

The problem is that moving on to intercept the communications of party B then picks up a whole range of other communications with parties C, D, E and so on. These people may be relatives, friends, business associates or even lawyers or members of parliament—and, of course, we are used to a privilege situation with lawyers and clients and members of parliament and we are concerned that that should always continue. They may be completely innocent parties and perhaps would not even know of the existence of party A, the person under investigation for whom the original warrant would have been issued, yet they are having their personal conversations intercepted.

What if these people, parties C, D, E and so on, are not so innocent? If they are involved in the same crime, the crime for which the original warrant was sought for party A, then that is fine; it seems a fair cop. They can be investigated as part of that. However, if the agencies suspect that these people are involved in some different crime, those agencies should not be allowed to use that sort of intercepted information to pursue those people. They should indeed be required to make new investigations into that new alleged crime and seek appropriate warrants based on evidence coming out of those investigations but certainly not based on their interception information relating to the party-A warrant. If we do not protect against this sort of indirect collection of interceptions from people for whom we have no warrant, then the infringement of individual rights and liberties would become untenable.

My concern then is that appropriate silos or firewalls are maintained between the person for whom this B-party warrant has been issued and any other person with whom they communicate. While B-party interceptions are currently provided for under the existing act, the Blunn report notes that it has not been utilised by enforcement agencies because the provisions on this matter were seen as being open to several interpretations.

What this legislation does is make it explicit that B-party services may be intercepted. It also gives certain protections, such as stating that B-party interceptions must be a 'last resort' and must be a last-resort recourse for law enforcement agencies—though it is always that last resort and the person who has the power to issue that last resort facility that is concerning. Nonetheless, many in our community have been alarmed by this proposal. Civil liberties groups have warned that B-party interception powers tip the balance too far away from our citizens' right to privacy and too far in favour of the ease and convenience of enforcement agencies in accessing their communications. This is a serious concern and one which the Blunn report noted. The report recommended that it be made 'clear that B-party services may be intercepted in limited and controlled circumstances'. It is not clear from my reading of this legislation that the circumstances will be limited and controlled enough to warrant spying on innocent Australians.

I certainly hope that the Senate Legal and Constitutional Legislation Committee will have a very close look at this provision, because this is an area where we must get the balance just right. We must not allow ourselves to become a people ever afraid. We should not be afraid of picking up the telephone or sending someone a text message or an email for fear that communication will be traced or listened to. We should not have to check what we say and censor ourselves because we do not know who may be listening.

The fact that we are considering the matter of B-party interceptions raises some broader issues that I would like to touch on. Before I do, I would say that many of these legislative changes have been made with an antiterrorist

intention and in an atmosphere and climate of new fears that pervade the world, including our country. It is important that people understand that the antiterrorist legislation itself widened powers so that there are already powers in our laws to deal with any interceptions if they are to do with a terrorist act or an imminent threat. The broader issues that I would like to touch on are important. The right to privacy is a right which is explicitly provided for under the International Covenant on Civil and Political Rights. The CCPR states:

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.

It also says:

Everyone has the right to the protection of the law against such interference or attacks.

Australia is a signatory to the CCPR and thus there is an obligation upon us to uphold the principles enshrined in it. However, the Howard government has repeatedly shown its disinterest in its international obligations. We have seen this in its treatment of asylum seekers—I note it is a year since Cornelia Rau was given her liberty and there has certainly been no payment of compensation at this stage; its treatment of working people, through its Work Choices legislation that has a new competitive edge which is about lowering people's wages and conditions; and its keenness to go to war in Iraq, where we have been for three years, no matter what the United Nations thought at the time.

International treaties and institutions do not mean too much to this government. I cite the daily revelations regarding the Australian Wheat Board scandal that links the Howard government closer and closer to the deception and cheating. To this government such international obligations can be treated as irrelevant to Australia with the claim that they impinge on our sovereignty or independence. Perhaps it is time that we took a cue from every other Western nation and actually enshrined some of the rights embodied in such international treaties as the CCPR in our own nation's law.

In this respect, I would like to draw the House's attention to the good work being done by New Matilda, who have proposed a human rights act to do just that. New Matilda should be congratulated for raising public debate about how such an act would help to ensure that all of the legislation proposed by this parliament meets the basic principles of human rights. It would be interesting to see how the B-party provisions of this legislation would stand up when measured against such a human rights act. I believe that some of this government's other legislation, such as that covering sedition and mandatory detention, would not pass muster under a basic human rights act.

I also believe that some of the statements made by the Prime Minister and others recently on Australian values would be more credible if they were backed by a concrete description of what our values are. In fact, there seems to be quite a deal of confusion between the Minister for Health and Ageing, Tony Abbott, the Treasurer, Mr Costello, and the Prime Minister himself on just what our values are. Apparently, it is a moveable feast. They are definitely ill defined by this government and are certainly subjective. A human rights act may be a way in which we can come to some kind of shared view on what our values actually are. It would spell them out in black and white, so that all Australians would have a clear indication of their rights and responsibilities. This is just a suggestion, which I believe is a good one, for ways in which we can use a human rights framework to help inform the community on these important matters. It would also help to inform us, as elected representatives, as we look at contentious legislation such as this which has the potential to infringe upon our human rights.

As I said earlier, there is a clear need to update the Telecommunications (Interception) Act to give our law enforcement agencies the powers they need to fight crime in this era of new and changing technology. I give full praise and commendation to the opposition for their efforts to bring better legislation into effect. However, any increase in these powers must be measured against the cost to the rights and civil liberties of our people, and we must be careful to get this balance right. There is no doubt that there are serious concerns about this legislation, and I look forward to a fuller examination of these concerns in the Senate committee process.