

## **Mail proposal goes 'beyond the pale'**

GEORGE WILLIAMS, DAVID HUME

24 March 2006

Hobart Mercury

THE Federal Parliament will next week debate a law that conjures up modern-day images of Big Brother.

The Bill will allow the government to read our private emails, SMSs and other stored communications without our knowledge. The power will extend even to innocent people, called B-Parties, if they have been unlucky enough to communicate with someone who is suspected of a crime or of being a threat to national security.

The government should sometimes be able to monitor the communications of innocent people. This may be necessary to protect the wider community where a suspect can only be tracked down through another person. However, the Bill goes far beyond what can be justified and undermines our right to privacy more than is needed to properly enforce the law.

Our key concerns are that, first, the government will be able to collect not only the communications between the B-Party and the suspect, but also communications between the B-Party and anyone else. If you are unfortunate enough to communicate with someone suspected of an offence (and, thereby, become a B-Party), the government may be able to monitor conversations you have with family members, friends, work colleagues, your lawyer, your doctor and so on, no matter what you spoke about. Your most private and intimate conversations could be pored over, without your knowledge, by people you have never met.

Second, in some circumstances, the government can use the information it collects even though that information is irrelevant to the original suspect. For example, if the government uncovers incriminating information from listening to a B-Party's conversations, this can set off a chain reaction allowing the interception of the incriminated person's communications or of anyone with whom they communicate. The government could use this information to initiate a prosecution, even if it relates to only a minor offence.

Third, the Bill sets a very low threshold for ASIO to be granted a warrant. As long as ASIO has tried other means of tracking a suspect, it only needs to show that intercepting the B-Party's communications is likely to assist in obtaining intelligence related to security. This is a very wide power particularly since, once ASIO meets the threshold, it can intercept any communications to or from the B-Party.

Fourth, the threshold that ASIO must satisfy uses general terms such as "likely to assist" and "relating to security". This vagueness creates the potential for government agencies to misuse the power or apply it in an arbitrary fashion.

This arbitrariness extends to another aspect of the Bill. The Bill differentiates between stored communications (like email and SMS) and real-time communications (like telephone conversations).

Under the Bill, it is much easier to access stored communications, apparently because SMSs and emails are thought to be less private than telephone conversations. However, now that telephone conversations often occur in public on mobile phones, many people, and particularly young people, reserve their most personal interactions for email and SMS.

These problems have been compounded by the speed with which the government has sought to push the Bill through Parliament. Interested parties were given only 10 days to prepare submissions on the 90-page Bill, and the Senate Committee responsible for reviewing the Bill has only two weeks to review the submissions, hear evidence and prepare a report.

The dangers of a bad process are especially high because, as just one part of a recent torrent of anti-terrorism legislation, it is easy for bad legislation such as this to slip by unnoticed and unamended.

Protecting our national security and investigating serious crime are important goals. However, we must be careful that in developing a legal response we do not lose sight of the rights and freedoms that we were trying to protect. We should ensure that, where the government is to gain intrusive new powers over our privacy, these powers are balanced and go no further than is needed.

This Bill for new surveillance powers over our emails and SMSs goes too far. It contains more power than is needed over too broad a range of innocent communications and contains too few safeguards. The government should go back to the drawing board to come up with a better proposal.

\* Professor **George Williams** is the director and David Hume an intern at the Gilbert + Tobin Centre of Public Law at the University of New South Wales.