Australian Privacy Foundation
post: GPO Box 1196
Sydney NSW 2001
email: mail@privacy.org.au
web: www.privacy.org.au

Telecommunications (Interception and Access) Amendment Bill 2008

Submission to the Senate Legal and Constitutional Affairs Committee

April 2008

The Australian Privacy Foundation

The Australian Privacy Foundation (APF) is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. We aim to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. We use the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed.

We have participated actively in the development of telecommunications privacy policy, including the changes to the Interception regime, being a regular contributor to Parliamentary Committee inquiries and official reviews

For further information about the Foundation, and previous submissions on the Interception regime, see www.privacy.org.au

Introduction

We believe that the Minister's assertion in his second reading speech that the Bill contains no new powers is incorrect. The changes to the device-based named person warrant regime to authorise the interception of communications made by multiple telecommunications devices clearly increases the access powers of enforcement agencies and reduces the level of privacy protection.

The proposed changes also need to be assessed in the context of the progressive extension of powers and loosening of controls and safeguards over telecommunications interception over the last 20 years. These previous changes, about which we and others have repeatedly warned and which in some cases are contrary to the advice of independent reviews (most recently the Blunn Report), mean that any incremental change such as those now proposed have an even greater potential impact than they would otherwise have done, or appear superficially to do. This is one of the corrosive effects of successive minor amendments, each apparently marginal and reasonable, but which cumulatively change the entire nature and impact of the regime.

Device-based named person warrants

The proposed changes would allow intercepting agencies to intercept communications on a potentially unlimited number of different devices used *or likely to be* used by a named person subject of a warrant. In the emerging telecommunications environment, this could be a very large number of devices, many of which will be shared by other individuals. We believe that the risk of intercepting agencies covertly accessing communications wholly unrelated to their investigations, and including communications between parties with no connection to their investigations, is too great.

We acknowledge the need for multiple device warrants as part of the investigative 'toolkit', but in our view, agencies should continue to be required to specify, and seek specific approval for, each device that they wish to intercept. This should not be unduly onerous as they will by definition have to identify each device in order to effect the interception, so the only additional burden is a minor administrative one. But that minor administrative

action of seeking approval of the issuing judge or AAT member for additional devices is in fact a major safeguard, and also a major deterrent against excessive interception.

The fact that previous amendments have provided for warrants to cover any 'telecommunications service' used or likely to be used by a named person subject should not be accepted as a valid precedent. We continue to believe that those changes removed important safeguards, and they should not become the default position in relation to devices.

The issues raised in the inquiry by the Committee into the 2006 amendments about the difficulty of uniquely identifying devices and services remain. The current proposals would appear to contradict the government's assurances in its response to the Committee's 2006 report, and no explanation is given as to how these issues have been resolved. We suspect that they have not been and that this Bill is simply an attempt to ignore them.

For more detailed arguments against the proposed amendments on device-based warrants we refer to, and support, the excellent submission by the Law Council of Australia, already published on the Committee's website.

Extension of sunset clause for exemption

The Bill seeks to extend the temporary exemption for agencies in respect of network protection systems, but no information has been provided on progress in developing a permanent solution that would avoid the need for the exemption. We note that the network protection issue is one which applies to businesses as well as government agencies and yet they have not been given the benefit of the exemption. We suggest the Committee opposes any extension without a progress report justifying it and explaining how the issue can be resolved for all organizations, not just Commonwealth agencies.

Reporting

The Bill seeks to change the reporting requirements, ostensibly to 'avoid duplication'. While on the face of it this seems sensible, we question whether it is desirable to cut the State governments out of the routine reporting loop in the way proposed. Keeping State Ministers informed of warrants is a useful safeguard - they may question them when the Commonwealth Attorney would not. No information has been provided about the views of the States on this change. The provision for 'optional' State reporting doesn't necessarily address the issue - State governments may well not take the trouble to 'opt-in' and then quietly forget all about the interception being done by their agencies - there is merit in our view having them 'force fed' the warrant information. While this cannot ensure that they apply an appropriate degree of scrutiny, the potential for them to do so is another important safeguard.

Any contact about this submission should preferably be by email to mail@privacy.org.au. Postal correspondence is re-routed and there may be substantial delays