Submission No 182

Inquiry into potential reforms of National Security Legislation

Name: Carly Nyst
Head of International Advocacy

Organisation: Privacy International
46 Bedford Row
London, WC1R 4LR
Great Britain

PRIVACY INTERNATIONAL

46 Bedford Row
London, WC1R 4LR
Great Britain
T +44 (0)207 242 2836
@privacyint
www.privacyinternational.org

Friday, 24 August 2012

Hon Anthony Byrne MP
Chair
Joint Parliamentary Committee on Intelligence and Security
Parliament House
Canberra
ACT 2600

Dear Mr Byrne,

Re: Inquiry into Potential Reforms of National Security Legislation

Privacy International wishes to support and reiterate the concerns expressed by the Australian Privacy Foundation in their submission to the Inquiry into Potential Reforms of National Security Legislation, dated 20 August 2012.

By way of background, Privacy International is an international human rights organisation, registered as a charity in the United Kingdom, with a network of partner organisations across the world. Founded in 1990, our mission is to fight unlawful surveillance and other threats to the right to privacy by governments and corporations. In addition to conducting extensive research and advocacy on privacy issues, we regularly advise and report to governments, corporations and international organisations, including the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development and various UN agencies.

Our staff, trustees and Advisory Board members have expertise on all matters related to communications access and interception. Recently, we provided evidence to two British Parliamentary Joint Committees on draft legislation that contemplates many of the issues raised by the Attorney-General's Department in their discussion paper to the Parliamentary Joint Committee on Intelligence and Security.

The concerns raised by the Australian Privacy Foundation in their extremely comprehensive submission are well-founded. The Attorney-General's discussion paper does not reflect any genuine consideration of the importance of balancing the need for Australia to improve its responsiveness to emerging and evolving security threats with the need to ensure that the right to privacy

of information and communications is preserved and protected. Not only do many of the measures suggested in the discussion paper threaten to erode pre-existing privacy protections and irreversibly lower legal thresholds, but much of the language used in the paper gives rise to the distressing inference that the Attorney-General's Department is urging the sacrifice of individual liberties in favour of unfettered controls that would contradict established human rights standards.

We wholeheartedly support the contentions made in APF's submission to the Inquiry, and particularly wish to emphasise a number of points.

Any laws or regulations which might infringe upon the enjoyment of the right to privacy must be necessary in a democratic society, and proportionate to their objective. Moreover, rigorous legal and judicial safeguards must be put in place to ensure that individuals are able to know, review, and contest decisions that affect the privacy of their information and communications. A number of steps proposed by the Attorney-General's Department are incompatible with these requirements. The lowering of the threshold for interception warrants (page 24 of the discussion paper) would drastically and disproportionately broaden the scope of police powers. The removal of fundamental accountability provisions (Item 10) would increase the potential for abuse of intercept powers. The extension of ministerial authorisations (Items 18a and 18b) would undermine the separation of powers and remove the important role of the judiciary in balancing individual rights against security interests. We thus reiterate Submissions 11, 16, 17 and 22 of APF's submission, and urge the Committee to ensure that rigorous legal and judicial safeguards remain at the heart of any communications policy going forward.

As APF urges, the government should approach cautiously any proposals to deputise the communications industry. A number of concerns arise when contemplating burden-sharing of surveillance arrangements; in particular, there is a real risk that the communications industry would obtain a level of protection from liability and immunity from accountability. At the same time, by imposing onerous technical and financial burdens on the industry, such arrangements may create disincentives to communications companies, particularly hindering innovation. We support APF's suggestions in Submission 14 and 15 that urge the Committee to give further consideration to both the practical and human rights implications of co-opting the communications sector.

Any legislative framework which hopes to adequately reflect and overcome the multitude of modern threats and challenges to communications integrity must recognise the risks of modern surveillance techniques that are currently being deployed around the world, and develop strong safeguards against their use and abuse. These include:

- The ability to remotely access computing and phone devices. Techniques and products exist that permit police to apply a Trojan against a computer or a mobile phone that will then result in the microphones being turned on,

cameras turned on, and all activity on the device to be recorded. In essence, this permits police to maliciously hack a device.
- The ability to access information on all mobile devices in an area. Through the use of devices including an IMSI-catcher, the police can enable the equivalent of a fake cell tower that will then get all nearby mobile phones to connect to the device. The device would then be able to access all the unique identifiers of all the devices, and cross match this against databases of account holders. This technique is advertised by the companies that develop the technologies as being particularly helpful for use at large public events and protests.
- The ability of authorities to track individuals by GPS.
- The ability of authorities to infiltrate online social media.

Legislative restrictions on the powers to monitor and intercept communications must be constructed in recognition of these capabilities. In this context, we reiterate APF's Submission 18.

Finally, data retention (page 10) of any service, sector, or type of provider is indiscriminate, impossible to secure against attack or abuse, and is thus a disproportionate infringement upon individual rights. In accordance with APF's Submission 19, the Committee should reject any proposal for new data retention requirements.

We urge the Committee to give serious consideration to the submissions provided by APF and other civil society actors. The lack of civil society consultation undertaken by the Attorney-General's Department prior to publication of the discussion paper is extremely concerning and reflects a fundamental lack of understanding about the importance of transparency and consultation in a process of legislative change in a democratic society. Accordingly, the Committee should, as APF submits, refuse to consider draft legislation that is not the result of a consultative process that reflects stakeholder's interests and inputs.

Privacy International would be happy to provide any further advice or guidance to the Committee if that would be of assistance.

Sincerely yours,

Carly Nyst, Head of International Advocacy