Australian
Privacy
Foundation

e m a i l: enquiries@privacy.org.au
w e b : www.privacy.org.au

29 April 2010

# Submission to the Joint Select Committee on Cyber-Safety regarding the Committee's Terms of Reference

## Submission by the Australian Privacy Foundation

## General issue

1. The Australian Privacy Foundation (APF) is the primary association representing the Australian public's interest in privacy. A brief backgrounder is attached.

2. We welcome the creation of a Joint Select Committee on Cyber-Safety and look forward to lending our support to the Committee's work where appropriate.

3. Further, we value this opportunity to provide input on the Committee's Terms of Reference.

4. This submission is intended to be made public.

## Privacy

5. We note that "breaches of privacy" is included in the Terms of Reference. This is important as various threats to privacy are among the most serious safety issues online, for people of all ages. Privacy is significant both in its own right and as an aspect of other personal information security risks, such as identity theft (also included amongst the Terms of Reference).

6. However, we are concerned about the one-dimensional approach to privacy hinted at by the fact that the Terms of Reference lists "breaches of privacy" as an aspect of "the nature, prevalence, implications of and level of risk associated with cyber-safety threats".

7. Privacy is a fundamental human right established through international law, so privacy also needs to be considered in the context of legitimate restrictions that should be placed on other measures purported to assist 'cyber safety'. This is because it has recently become all too common to justify government or corporate measures which undermine privacy on the basis of a sometimes amorphous ambit claim about the need for 'security'. While there are extensive legal loopholes supporting necessary and practical law enforcement and other exemptions from certain privacy protections, it is important to recognise that, from the perspective of the citizen, 'the cure can be worse than the disease'. Many threats to privacy and other human rights and civil liberties arise from overzealous or unsubstantiated assertions about the demands of 'security'.

8. For example, the right of privacy places limits on surveillance and investigation measures used to pursue cyber safety.

9. In other words, the right to privacy, while an aspect of cyber safety in many cases, is also likely to require assessment of the necessary and reasonable limits on what steps should legitimately be taken in pursuit of 'safety' online.

10. For instance, technical measures which monitor the content of user-originated or -received packets (Deep Packet Inspection) or of client-side requests of servers on the Internet in order to censor and block access to deprecated items creates the technical capacity for ubiquitous, invisible and poorly governed surveillance. The existence of the transaction logs of such monitoring, which would for instance be necessary to implement many models of ISP-level filtering, raises questions about the use of this information in other 'security' activities such as law enforcement investigation. We should not easily and without deep hesitation embark on a scheme which implements the infrastructure of universal surveillance for law enforcement purposes in the name of safety.

11. A related concern is the incremental expansion of the matters that are deprecated in the name of safety, security or law enforcement. For instance, because Australia lacks the balancing privacy-enhancing protections taken for granted in the US, such as for free speech utterances (in the First Amendment to the US Constitution) or 'fair use' of information (in copyright law), it is a matter of concern that there are proposals (including in the proposed, secretively-developed ACTA treaty) to adapt Internet infrastructure for the purposes of enforcement of international commercial interests.

**Privacy and Young People**

12. Different models of the vulnerabilities, capabilities and needs of young people point to different ways of protecting their assumed interests. We suggest encouraging in young people a fundamental lifelong respect for their own and other people's privacy against unwanted intrusions from any source, including government and business as well as 'criminals'.

13. This approach would focus on less intrusive rather than more intrusive technical and legal measures (for the reasons above), and adopt the emerging consensus that building individual 'resilience' and self respect in the face of any current or future challenge online is more likely to be in young people's long term interests than a series of controversial, partial, quickly obsolete and ineffective technical measures, or draconian but rarely used 'law and order' provisions adding to the already very heavy criminalisation and prohibition of a wide range of online activity.

## What is cyber safety? What interests should be protected, how?

14. The analysis of potential 'harms' on the net, how they affect the interests of various groups who may have a claim to 'protection', and the relative value of various legal, technical or social options for protecting these interests, is incomplete and controversial at present. While there may be consensus on some issues or ways of characterising certain problems, other perspectives are disputed and surrounded by ambiguity and rhetoric as much as reasoned discussion and objective consideration of evidence, or the lack of it. Proceeding on the basis of assertions, slogans, thinly veiled political or religious agendas or received wisdom is unlikely to assist those who have a legitimate claim for protection, because the online environment is dynamic, ubiquitous and not well understood, It is important that this inquiry acknowledges and articulates the range of views, unresolved categorisation issues, and also the and potential implications, limitations and unintended side effects of various, often well-meaning proposed interventions.

15. Acknowledgement that a suite of solutions or measures is required, or that a particular solution is 'not a silver bullet', should not distract attention from reviewing the specific costs, risks and benefits of each proposed solution compared with all the others. Those which have excessive or unknown costs or risks compared to any demonstrated benefit should not be proceeded with as part of some suite.

**This matter needs more serious and substantial attention**

16. The evidence and analysis base in the area of online content, including the classification and content regulation model at the heart of it, and the implications of emerging issues such as 'user generated content', the 'death of the publisher' and ubiquitous communications devices, is inconclusive and incomplete. The current models are complex, inconsistent between media and jurisdictions, and ad hoc. Questions in this area are however a core concern for the current discussion about cyber safety.

17. A much more robust review and more research is warranted before any fundamental decisions are made on reconstructing the overall scheme of protecting the interests of people, including young people, online. The short notice for this inquiry, and the lack of timely publicity, media information, information about public hearings or background information are signs that not enough attention, consultation or substantial thought has been applied to this matter yet. This builds on the lack of adequate engagement with the proposal for an ISP filter to censor access to online material, which has not been subject to a Law Reform Commission report, a full parliamentary review, or extensive work on the fundamental interests involved or alternative options. This current short, under-resourced and -publicised inquiry cannot remedy such defects; it should be a first step on a serious assessment, not a hasty stamp of approval on some as yet unspecified package of options.

18. It is better, for both privacy and the wider interests of young people, to take the time now to get it fundamentally right for a long term stable and adaptable regime than to continue with the ad-hoc, poorly integrated, inadequately consulted, often very politicised practise of the last decade or so. It would be inappropriate to proceed with substantive legislative change or the commitment of substantial funding based on existing limited, controversial and confused models. Greater clarity, openness and rigorous analysis and assessment of both risks and comparative efficacy of solutions is required before such steps.

19. The APF looks forward to working with the Committee in the pursuit of these goals.

For further information contact:

Vice-Chair David Vaile, 0414 731 249
Vice-Chair Dr Dan Svantesson, (07) 5595 1418
E-mail: enquiries@privacy.org.au
APF Web site: http://www.privacy.org.au

**Australian Privacy Foundation**

**Background Information**

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF's Board comprises professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by a Patron (Sir Zelman Cowen), and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87)
  http://www.privacy.org.au/About/Formation.html
- CreditReporting (1988-90)
  http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07)
  http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-)
  http://www.privacy.org.au/Campaigns/Media/