Australian Privacy Foundation

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

w e b : www.privacy.org.au

5 July 2010

Submission to the Joint Select Committee on Cyber-Safety

Submission by the Australian Privacy Foundation

Introduction

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, with particular focus on the selected topics currently in the Committee's focus..

4. This submission is intended to be made public.

5. Summary

- Privacy, and personal information security, is a critical component of 'cyber safety'.
- Online privacy should be considered in a broader context in cyber safety discussions
- Meaning and scope of 'cyber safety' is unclear. Distinction from 'cyber security' makes sense for government, but distracting for individual – online threats cross boundaries.
- 4 sources of threats to your safety, personal information security and privacy online:
    i. You yourself, and your online 'friends' and contacts
    ii. Criminals and fraudsters, malicious or negligent strangers, etc. ("baddies")
    iii. Corporate entities with business models in conflict with your interests
    iv. Governments unwittingly undermining the civil society they seek to support
- Important to recognise that some 'cures' may be worse than the disease: heavy handed government solutions may undermine personal information security and privacy online.
- Fundamental investigation of risks, options, consequences, costs, and alternatives has not been done or is incomplete. There is no clear case for responses which are expensive, unproven or inherently prone to risks of unintended consequences.
- Technological measures like ISP level censorship filters may have political attraction (some people may wishfully think they will somehow 'make the unpleasantness go away') but are clouded in 'spin', controversial, and unproven -- potentially dangerous for privacy and personal information security for little benefit.
- Technological 'fixes' may paradoxically even make things worse than doing nothing, if they offer false security, but interfere with sustaining the trust needed to build resilience.
- More promising, safer, future-proof options focus on education and resilience building – how to do this well is also not well established, needs more investigation and research.

Privacy and 'cybersafety'

6. 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).

7. However, we are concerned about the relatively 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". Our concern is amplified by the fact that "breaches of privacy", as one of select topics, is focused on as it "relates to children and young people", rather than as would be appropriate, in a broader manner.

8. We note also that a practice developed of differentiating between 'cybersafety' (apparently relating to personal interactions online, and issues arising from access to certain content, and those behind such content) and 'cybersecurity' (understood to focus more on vulnerability to threats from organised crime in relation to fraud, network intrusion, and computer hijacking). While there may be some benefit for some purposes in this distinction, especially from a government perspective, there is also potential for unnecessary territorial or jurisdictional rivalry interfering with a clear focus on the needs of the online 'end-users' (a.k.a citizens, consumers, individuals) for whose interests we advocate. Privacy and personal information security issues underlie both aspects of online life, with some technologies and practices overlapping both, and it may be better to focus on these issues wherever they manifest rather than on such distinctions.

9. 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 critical in this context, 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' in general terms, which is assumed to by default over-ride all other considerations in principle, often with limited consideration of cost/benefit, evidence of actual benefit or threat, or consideration of less intrusive means to support reasonable safety and security. While there are extensive legal loopholes in privacy law supporting certain necessary and practical law enforcement and other exemptions from particular privacy protections, it is important to recognise that, from the perspective of the citizen, 'the cure can be worse than the disease'.

10. Many threats to online privacy, and other human rights and civil liberties, arise from overzealous or unsubstantiated assertions about the demands of 'security'. And some of the solutions, by potentially offering a 'false sense of security' (sometimes uncritically accepted by a media and public only too happy to think there is a mechanistic or simple solution to complex, dynamic and uncomfortable social problems), may paradoxically make things worse -- by diverting attention from

11. In light of this, the Committee must constantly be aware that the right of privacy properly places limits on surveillance and investigation measures used to pursue diffuse notions of 'cyber safety'. While specific investigations of particular offences or identified imminent threats may in some cases warrant one-off action to bypass certain protections, this exception model should not be extended into a generic deprecation or abandonment of the default entitlement to live life online without fear of being routinely treated as a suspect without any right to privacy.

12. In other words, the right to privacy, while an aspect of cyber safety in many scenarios, is also likely to require assessment of the necessary and reasonable limits on what steps should legitimately be taken in pursuit of 'safety' online. While recently government figures have cited concerns about alleged abuses of privacy by online businesses like Google or Facebook, it is important to recognise that government itself may also constitute a serious threat to personal information security and privacy.

13. 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 may create the technical capacity for ubiquitous, routine, invisible and poorly-governed surveillance. The existence of the transaction logs of such monitoring, which would for instance be necessary to implement some models of ISP-level filtering, raises questions about the potential use of this information in other 'security' activities such as law enforcement investigation.

14. 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'.

15. A sober and open examination of evidence should precede any decision to pursue the introduction of such technologies. This would extend the current review and ask about the full range of real 'cyber safety' hazards and their relative incidence and seriousness, whether proposed solutions would have any actual ongoing effect on the particular threats they are assumed to address, the potential for unintended costs, risks and "scope creep" for each proposed solution, the potential of alternative less intrusive solutions, and the priority that should be accorded the various hazards and solutions.

16. A related concern is the incremental expansion of the matters that are deprecated in the name of online 'safety', 'security' or law enforcement, to include assertion of private rights by administrative means. There is a growing tendency to bundle an ever wider range of interests together and treat them as if they all warrant the same degree of relaxation and undermining of civil liberties and individual rights which pursuit of eg., serious violent crimes would. 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 secretively-negotiated proposed ACTA treaty) to adapt Internet infrastructure for the purposes of enforcement of international commercial interests.

17. Official assurances about the benign nature of such secret negotiations cannot be given much weight, as the capacity for civil society to participate, observe and contribute to such exercises dominated as they are by professional lobbyists for commercial interests, is deliberately negated. Privacy-intrusive legal or practical outcomes will be difficult to reverse once agreed behind closed doors.

18. It is important to re-think what we mean by 'cyber safety', and reaffirm that 'cyber safety' includes being able to participate in a wide variety of normal activities online without the constant fear of one's 'data trail' being made routinely available for various government or private stakeholders to use adversely in ways which potentially deny both natural justice and privacy.

19. (This includes considering the impact of 'cloud' based services on our ability exert jurisdiction over those responsible for such abusive practices; and similarly, the potential erosion of the role of our ISPs as our 'common carrier' style servants and their incremental conversion into the unpaid agents of such government and private stakeholders, adverse our privacy interests.)

Privacy and Young People

20. Different models of the vulnerabilities, capabilities and needs of young people point to different ways of protecting their assumed online interests. We suggest a key solution lies in encouraging in young people a fundamental life-long respect for their own and other people's privacy and personal information security against unwanted intrusions from any source, including from government and business as well as 'criminals', or even their 'friends'. This is sometimes called 'building resilience'. While it may appear less dramatic and 'tough', it is a better basis for frank discussion, limiting the damage of future cyber safety threats, and sustaining civil society compared with the 'security'/technical model that assumes outside agents and barriers can effectively 'protect' young people from all harm. Online content and technical threats are evolving so rapidly, and countermeasures are so easily outmoded and outpaced, that exposure to online threats is unavoidable; the real issue for cyber safety is how to minimise the impact of this exposure, which is a feasible goal, rather than how to reliably prevent it, which is not.

21. 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 current or future online challenges 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?

22. 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. Current proposals, for instance for the mandatory ISP level black list content censorship 'filter', have been developed and debated without the normally expected level of fundamental investigation of issues such as the nature of the various purported harms, the limits and application of various remedies and regulatory models against current or future versions of those harms, and comparisons with alternative options.

23. 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, or 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, and potential interventions in it, are dynamic, ubiquitous but not well understood, it is important that this inquiry acknowledges and articulates the range of views and unresolved categorisation or classification issues; and also the potential implications, limitations and unintended side effects of various, often well-meaning proposed interventions.

24. Acknowledgement that a suite of solutions or measures may be required, or that a particular solution is 'not a silver bullet' (which may deflect proper scrutiny on whether it has any value at all), should not distract attention from reviewing the specific costs, risks and benefits of each proposed solution compared with all the others. Those proposals which have excessive or unknown costs or risks compared to any demonstrated benefit should not be proceeded with as part of some suite, even if there is an emotional case to be seen to be 'doing something'.

25. As noted above, many of the advocates for young people's interests online appear to focus on the means for encouraging awareness and influencing risky behaviour in young people. This educational approach has much to commend it, particularly if it results in further investigation about how the often obscure privacy risks created by online activity can effectively be brought to the attention of young people in a way which actually has an impact on their behaviour. A balanced, frank account of 'rights and obligations - risks and benefits' of Internet use when young people are offered access to school computing systems would be one potential contribution. However, even more important is to develop these options using a methodology that focuses on whether they work and 'cut through', and how to incrementally improve their effectiveness in bringing privacy and personal safety protection behaviour into the mainstream of young people's thinking. This may require review of whether current approaches are working for the end users, or serve other goals such as institutional promotion, or re-assuring parents.

This matter needs more serious and substantial attention

26. The evidence and analysis base in the area of online content and 'safety', including the classification and content regulation model at the heart of it, and the implications of emerging issues such as 'user generated content' (replacing a centrally controlled, low volume distribution system susceptible to traditional censorship and classification with an exponentially high volume one where each person can become a creator, consumer, distributor and classifier), the 'death of the publisher', and ubiquitous smart communications devices, is inconclusive and incomplete.

27. The current regulatory models are complex, confusing, often arbitrarily inconsistent between media and jurisdictions, and ad hoc. Questions in this area are however a core concern for the current discussion about cyber safety.

28. The current inquiry is a start, but it covers a very wide range of territory in a very limited time frame, apparently for political purposes to support the early implementation of schemes which in fact need a lot more work. A more robust fundamental review and more relevant, publicly accessible independent research is warranted before any fundamental decisions are made on reconstructing the overall scheme of protecting the interests of people, including young people, online. A thorough and balanced discussion about what 'safety' means in the current and future online environment would be a first step, with privacy and personal information security matters a key component.

29. 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 quite politicised practices 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.

30. 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
- Credit Reporting (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/