Submission to the Senate Standing Committee on Environment, Communications and the Arts

regarding

Online Privacy

There is no doubt that computers and telecommunications have dramatically increased the possibilities for privacy to be breached. Such breaches can arise due to the actions of various other parties, such as organized crime groups, opportunistic individuals, lax companies and over-zealous marketing organizations.

However the Rudd and Gillard governments have done more than a legion of cyber-criminals have been able to do in putting Australians at risk of privacy breach. The record so far is not pretty.

1. The Rudd government attempted to water down the provisions of the *Telecommunications (Interception and Access) Act*, which is the front line in the fight against deliberate breach of privacy via telecommunications. Eventually the government backed off from most of the weakening of the privacy provisions in this Act.
2. The Gillard government continues to attempt to introduce internet censorship.
    - At the heart of any internet censorship system is wide-spread examination of the URLs that each user is accessing, with a view to allowing some requests through and disallowing others. With this infrastructure in place it will be trivial to add monitoring and logging of each URL accessed. Such capability may well be present in many Commercial Off The Shelf censorship products from Day 1.
    - This vast store of information will be a tempting target for idle ISP employees, rapacious marketing companies, cyber intruders, and prying governments.
    - A URL may actually contain private information i.e. over and above the fact that it was accessed.
    - The internet censorship mechanism itself presents a tempting target for a malicious external party, for the purposes of breaching privacy ... or worse.
    - Few would believe that internet censorship, once implemented, would remain limited to one protocol (HTTP, the protocol used to implement the web) or one classification (Refused Classification, or whatever the Gillard government might attempt to introduce initially), if indeed there are any legislated limits from Day 1.
3. The Gillard government has canvassed a proposal that would require ISPs to operate wide-spread surveillance and recording of all or much of their customers online activity, in case the government needs it at some time in the future.
    - The government refuses even to be open about what this proposal involves, on the grounds that to do so would provoke "premature unnecessary debate". Newsflash ... the debate is happening anyway - so the government might as well either come clean with the Australian people or abandon the whole idea.
    - This proposal would likely extend the breach of privacy from the area of web pages accessed into the area of email.

    - As above, this proposal would create a store of information that would be a tempting target and the collection mechanism itself would increase the risk of a privacy breach.
4. While not pertaining to the Australian government, I read in recent days that the US government has released proposals to render useless all encrypted network protocols. This would turn the clock back decades to the days when encryption algorithms had to be exported printed on tee-shirts. The existence of deliberate "holes" in encrypted network protocols would create both a risk of privacy breach by government and a risk that the weakness is exploited by a third party.

Excluding the egregious plans of the Gillard government and other governments, privacy breaches are often contributed to by the person in question. This may arise from many sources.

1. People simply have different standards of what is appropriate privacy i.e. the person would not consider it a breach.
2. People may not clearly understand what a privacy breach can lead to e.g. identity theft.
3. People may have poor security practices that lead to the compromising of their computer i.e. information was not explicitly or intentionally released.
4. People may not give adequate thought to whether information should be disclosed e.g. time poor.
5. People may be tricked into disclosing information e.g. social engineering.
6. Software may be configured with default settings that do not adequately protect privacy.

Government can contribute to improving the privacy of Australians.

- The most important thing that the government can do is to **back off** from its intrusive proposals for internet censorship and internet surveillance.
- Just in case you missed the point ... **the single biggest threat to online privacy today is being created by governments.**
- Government should be involved in educating people about risks and consequences of privacy breach, what to do in order to avoid it and what to do if it has happened. This particularly applies through the education system where children can be helped to develop appropriate behaviours from a young age.
- Today we have the farcical situation where one part of government is advising people to use a proxy in order to access web sites with greater privacy while another part of government is pushing to introduce internet censorship that will be bypassed by a proxy.
- Government may set standards for information handling by companies, and get involvement by companies either through draconian enforcement or voluntary certification or a combination of the two.
- About the best I could say for the government's proposals for internet censorship and surveillance is that those proposals will surely spur the development of better tools to protect online privacy, albeit that that is presumably the exact opposite of the government's intention. Unfortunately, as now, only those who are motivated will be able to protect themselves adequately