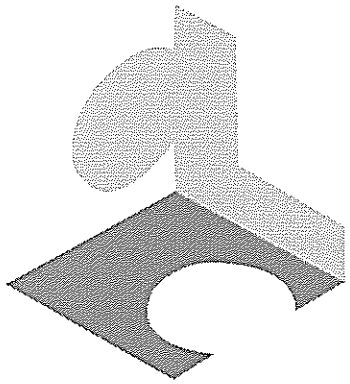
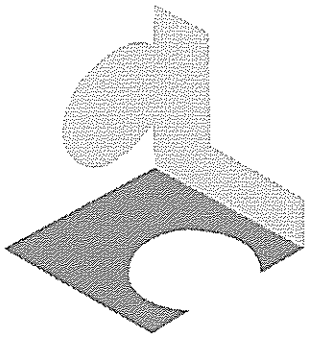


Communications Law Centre, UTS

Submission to the Joint Select Committee on Cyber-Safety

Inquiry into Cyber-safety of Senior Australians

22nd March, 2012



Communications Law Centre, UTS

1. Recommendations

1.1 Senior Australians to play an active role in training and educating other seniors on the benefits of internet and the dangers of cyber-crime;

1.2 The creation of a 'cyber-notary' to act as an intermediary for vulnerable and reluctant internet users;

1.3 Improved reporting of cybercrime, including centralised reporting capability;

1.4 Leadership on cyber-safety to devolve to a single government body;

1.5 Compliance with any ISP industry code to be mandatory;

1.6 Improved efforts to overcome the online anonymity of cyber-criminals;

1.7 Law enforcement agencies to lead the development of technical, social and legal infrastructure that prevents the opportunity for cyber-crime;

1.8 Greater international cooperation to solve the problems of investigative efficiency, jurisdiction and extradition.

2. Introduction

2.1 The digital revolution has provided all Australians with tremendous opportunities. These opportunities can be felt in all aspects of life from social connection, education, access to services and business possibilities. To benefit from these opportunities, individuals must have confidence in navigating the online world. This confidence will arise from a combination of experience online and gaining specific knowledge of the potential threats that exist online. Confidence and mastery of the online world will, naturally, also benefit from reducing the threat of cyber-crime. This challenge will continue to be our first priority, and will require the cooperation and combined will of government, business, citizens and the international community.

2.2 All Australians are at risk of cyber-crime and in an ideal world we would have the capability to eliminate that threat. However, there are many obstacles to overcome in order to make online world safe for all to navigate. Improvements need to be made in the areas of ISP responsibility; the reporting of cyber-crime; the investigation of cyber-crime (made difficult by the problem of the online anonymity); 'high tech policing' by law enforcement agencies leading a collaborative effort that involves input from the IT industry, business and financial services and other relevant groups aimed at designing systems that are protected against cyber-crime; international cooperation with respect to information sharing, extradition and questions of jurisdiction.

2.3 These are areas that need urgent attention. However, as much as we might try to eliminate the threat, cyber-crime is likely to remain with us in some form and it is also likely to evolve as efforts to curb cyber-crime become more effective. In society, some people will also continue to be more vulnerable than others. The CLC acknowledges the work done by a number of government agencies and other bodies that dedicate resources to tackling the problem of cyber-safety. It is important that advances in this area continue to evolve in order to ensure that messages regarding safe conduct translate into behavioural change. We also need to be able to find ways to measure the success of government programs.

2.4 Most importantly, we also need to feel confident that benefits of educational initiatives in fact reach those who are most vulnerable in order to ensure that all Australians have equal access to the opportunities of the internet.

3. Issue 1: the nature, prevalence and level of cybersafety risks and threats experienced by senior Australians, and

Issue 2: the impact and implications of those risks and threats on access and use of information and communication technologies by senior Australians.

3.1 The CLC notes that evidence on the impact of cyber-crime on seniors tends to be more anecdotal than empirical. The evidence that does exist in fact tends to suggest that there is no clear correlation between a person's age and susceptibility to cyber-crime. With respect to the confidence of Australians online, ACMA research suggests that *ability to manage security of personal information*

online increases the more individuals use the internet[1]. Those who used the internet the most (over 15 hours per week) were the most confident, with 60 per cent of respondents indicating that they were either *fairly* or *very* confident, and those who use the internet the least (under 7 hours per week), were the least confident, with only 45 per cent of respondents indicating a similar level of confidence. By contrast, this report indicated no significant difference in confidence levels according to age group.

3.2 This finding seems to support a common sense assumption that the more time people spend online, the more comfortable they are likely to be when it comes to engaging in online activities. Whatever the realities may be with regards to incidents of cyber-crime as categorised by age group, it is important that confidence in the technology in encouraged. The role of government and institutions should not merely be to warn about the risks, but to encourage usage. It is through a positive experience online that all Australians will derive the benefits of the internet age.

3.3 We also note, however, that while all Australians are potential targets of cybercrime, seniors have been identified as being more susceptible to particular types of cybercrime – in particular, investment scams. Senior Australians are often targeted because they have money to invest as they approach retirement. We note that such crime exists as much in the offline world as the online world. The digital world has merely amplified the means by which fraudsters can connect with targets.

4. Issue 3: the adequacy and effectiveness of current government and industry initiatives to respond to those threats, including education initiatives aimed at senior Australians.

4.1 The CLC believes that senior Australians themselves have an important role to play in creating a safer online environment for other seniors. Many senior Australians are savvy internet users, with years of experience online, and they are well placed to engage with other seniors regarding relevant experience, advice on how to navigate the internet, how to take advantage of services available on the internet, as well as providing advice on cyber threats.

4.2 The CLC acknowledges the good work done by the Australian Seniors Computer Clubs Association (ASCCA) in promoting online education for seniors. We support the objectives of ASCCA whose broad purpose is to 'broaden the vision and understanding of available technology and what is possible'[2], as well as to provide warnings about cyber threats. We believe this is the right approach. Gaining knowledge about the problems of internet usage should be understood alongside an appreciation of the advantages. The purpose of education is to instil confidence, not to inspire fear.

4.3 The CLC also notes the findings of ACMA commissioned report on international cyber-safety campaigns[3]. Key findings of this report are that:

---

[1] ACMA (2010), *Digital Australians – Expectations about media content in a converging media environment,* pp68-70

[2] http://www.ascca.org.au/index.php?option=com_content&view=article&id=69&Itemid=168

[3] ACMA (2011), *An Overview of International Cyber-Security Awareness Raising and Educational Initiatives,* p6.

- The most successful projects are ones that integrate information with training and skill acquisition. Skill acquisition may take place through formal training programs, online quizzes, video games, and formal curriculum assessment;
- Many organisations have found the most cost-effective way to produce positive results is to keep a project simple and focused on a target group.

The report makes clear that a number of projects falsely assume that if a user acquires information of Cyber-Security that this will automatically translate into more secure conduct online.

4.4 Interactivity and targeted resources are at the heart of the ACMA's innovative Cybersmart program which is direct towards children and parents. The CLC believes that a similar initiative directed at senior Australians merits attention and might adopt a similar approach with respect to encouraging a 'hands-on' and interactive experience. We note, however, the finding of the ACMA's international report that, 'host organisations find it challenging to evaluate the effectiveness of education and training initiatives – qualitative and quantitative metrics are difficult to put into place for such initiatives'[4]. Clearly, any government initiative that aims to educate senior Australians on the dangers of the internet would benefit from a capability to measure the results of the program with respect to the 'real world' conduct of seniors online. A program to help senior Australians with computer literacy may wish to take advantage of the many volunteer clubs and organisations throughout the country in promoting and implementing the program.

4.5 The CLC also recognises that despite educational initiatives, some Australians may remain mistrustful of the internet, or simply refuse to go online. As services increasingly move online, this will put a large number of people at a significant disadvantage. The CLC suggests that consideration be given to a public service to enable such people to gain access to services through an intermediary.

Issue 4: best practice safeguards, and any possible changes to Australian law, policy or practice that will strengthen the cybersafety of senior Australians.

Reporting and institutions

4.6 It appears to the CLC that victims of cyber-crime have difficulty in accessing law enforcement. It seems that state and federal police are limited in their ability to receive, process and respond to requests for assistance from citizens. These limitations need to be addressed. The CLC also supports the creation of online crime reporting capacity that enables victims of cyber-crime to easily report crime to police and regulators. This centralised reporting capability must allow a broad definition of 'cyber-crime' to include all offences that are facilitated online, not just those associated with malicious code.

4.7 The CLC is aware of the good work done by the AFP, the ACMA, the DBCDE and the ACCC in tackling different areas of cyber safety. However there are likely to be gains in efficiency, public access and comprehensiveness of approach, should one body take leadership of what is a 'whole of society' problem.

---

[4] *Id*, p6.

ISPs

4.8 The CLC believes that ISPs should play a more active role in ensuring that their networks are free from malicious code. This should certainly extend to code that the ISP knows, or ought to suspect, may contain harmful code for end-users. The CLC notes that this recommendation should be seen as part of a broader ongoing debate about the responsibilities of digital providers. The question must be addressed, whether ISPs should be allowed to continue to act as 'mere conduits' for illegal activity?

4.9 The CLC believes the voluntary ISP code of practice (iCode), introduced in late 2010, represents an important first step by which ISPs adopt a level of responsibility for the content to which they facilitate access. It represents something of a paradigm shift in the attitudes of ISPs – in that there is acknowledgement that there are options available to ISPs to reduce threats – it only requires the will to execute those options.

4.10 However, the CLC believes that compliance with any industry code should be mandatory. There also need to be appropriate and proportionate sanctions that reflect international developments.

Identify cyber-criminals

4.11 Setting aside all aspects of domestic law, jurisdiction and enforcement, the greatest challenge in the effort to curb cyber-crime is the sheer difficulty involved in tracking down a suspect. The main reason for the difficulty is the ease by which online individuals remain anonymous and the difficulty of locating the origin of the crime. By the time international efforts can be gathered, and jurisdiction is settled upon, the cybercriminal has the opportunity to disappear into the fluidity of cyberspace.

4.12 The CLC believes that we must apply attention and resources on the issue of online anonymity in order to find an effective technical solution to the problem of investigating cybercrime.

High level strategy

4.13 The work in developing a high level strategy needs to be a joint initiative between law enforcement agencies, security companies, business, consumers, software and hardware providers, ISPs and other stakeholders. Law enforcement agencies must play an active role in leading the development of technical, social and legal infrastructure to build to a safe online environment. The problem is highly complex, and the CLC believes that law enforcement agencies should adopt a 'customer relations management' approach to the problem that takes into consideration strategic information from IT security companies, business and industry, financial services, IT companies, online citizens and consumers and consumer groups, in order to address cyber-crime by establishing standards which make the internet itself more secure by reducing the opportunity for cyber-crime.

International cooperation

4.14 Cyber-crime does not respect international boundaries. A threat is just as likely, if not more likely, to come from code sent from a server located overseas, as it is to come a server within state boundaries. This represents a problem not only of jurisdiction, but problems of identification of criminals, enforcement and information-sharing between agencies.

4.15 Concerns over national sovereignty have limited attempts to cooperate on international criminal investigations in the past. However, since the threat of cybercrime to international security is so

profound, we cannot afford to take our time. Governments must also consider opening channels in order to exchange information and gather information in a timely way.

4.16 The CLC points to the international effort in closing down the Mariposa botnet threat in 2009, which lead to the establishment of the Mariposa Working Group – a cooperative effort between Defence Intelligence, Georgia Tech, Information Security Center, Panda Security and other international security experts and law enforcement agencies.

4.17 Clearly, the domestic laws of nations would benefit from harmonised laws that would criminalise certain conduct, reduce interjurisdictional conflict and allow greater international cooperation. Establishing a framework for greater international cooperation is essential.

4.18 The European Convention on Cybercrime is an important attempt at harmonisation and resolving interjurisdictional conflicts. However, it is just a first step and it requires ratification from all the major international players. Currently, Russia, a hub of cybercrime activity, and China, an apparent hub of cyber-espionage, are yet to sign or ratify the Convention.

4.19 The CLC also notes that the Convention has no impact on extradition treaties, which remain bilateral and subject to domestic law.

Yours Sincerely,

Professor Michael Fraser, AM
Director
Communications Law Centre, UTS

Mark Briedis
Researcher
Communications Law Centre, UTS

William Renton
Researcher
Communications Law Centre, UTS