7

Concluding comments

7.1 The internet has become an essential tool for participation in many aspects of modern life. Australians, including many seniors, are online for business and pleasure, for social networking, accessing government information or education, for shopping and other financial transactions. Unfortunately, there are many seniors who are not taking part in the digital revolution. The reasons for non-participation are various, but fear of becoming a victim of cybercrime is a real deterrent to many seniors.

7.2 The immediacy and global nature of the internet, and its convergence with new technologies such as smart phones and portable tablets, offers expanded opportunities for communication, education, health services and business. However, as government and businesses embrace online interaction to diversify and improve their services, criminals are embracing new opportunities in the expanding market to commit a host of cyber-enabled crimes.

7.3 Keeping seniors cybersafe requires a multi-faceted approach. The Australian Federal Police (AFP) told the Committee that to achieve a high level of cybersafety for all Australians, we need the right mix of law enforcement, policy and legislation, education and also some level of user vigilance.[1] The Department of Broadband, Communications and the Digital Economy (DBCDE) made the same point:

> Internet security is a responsibility shared by all who engage in the online environment. While government efforts to create a safe and secure online environment span regulation, enforcement, education and awareness raising and international engagement,

---

1 Australian Federal Police (AFP), *Submission 20,* p. 5.

ultimately it is businesses and individuals who must take responsibility for their own safety and security online.[2]

7.4   It is crucial, according to the AFP, that seniors are equipped with the necessary knowledge and skills to use information and communications technologies safely.[3]

7.5   The Committee found that our existing laws relating to cybercrime are currently going through a period of review and reform to meet the challenges posed by technology advances and developments in cybercrime. The Committee believes the case was well made during the inquiry for on-going, progressive review of relevant cybersafety laws.

7.6   The Committee was very impressed by the efforts of seniors' groups and libraries around the nation which are teaching seniors how to use computers safely so that they can enjoy the benefits of being online without unnecessary fear. These seniors' groups and the libraries told the Committee that they could do much more if they received funding to do so. The Committee has made a recommendation to government to find a way to support these groups and the public libraries to increase this valuable role that they play.

7.7   Problems of access, cost and training need to be addressed if all senior Australians are to have reasonable access to the many benefits of using the internet. The President of the Australian Seniors Computer Clubs Association aptly summed up the message delivered by so many stakeholders to the Committee:

> We must protect [seniors]…as they try to achieve access and equity in this age of technology. Seniors may be one of the fastest growing age groups taking up the use of the internet, but they still represent far too low a percentage of that community…education and skills training [is] essential…The NBN has the potential to bring great opportunities to all Australians, but seniors need to be educated and informed so that they can use a computer and access the internet safely. They must be helped to understand how to protect and secure their computers by being able to identify online security threats, make transactions securely online and help their families to be safe online. Education is badly needed.[4]

---

2   DBCDE, *Submission 25*, p. 8.

3   AFP, *Submission 20*, p. 5.

4   Mrs Nancy Bosler, President, Australian Seniors Computer Clubs Association (ASCCA), *Committee Hansard*, 23 March 2012, p. 15.

7.8   In the Committee's previous report, *High-Wire Act Cyber-Safety and the Young*, the Committee stated that it took a lot of evidence calling for a national co-ordinated approach to cybersafety. This continued to be a concern which was raised often during the current inquiry. Telstra, for example, said:

> A holistic approach to cyber-safety is required to empower all Australians to exercise reasonable care and responsibility in their online activities [and] the key components of this holistic approach include education, legislative protections, law enforcement, international co-operation, appropriate products and [for children] parental supervision…A smart, ethical and socially aware online experience requires individuals to adopt responsible online behaviours; and effective education and awareness programs are needed by whole of government to establish a broad sense of inclusion, responsibility and community to drive the change in online behaviour.[5]

7.9   The Committee took a lot of evidence seeking the establishment of a centralised access point for information and crime reportage, with follow-up support for victims where needed. Currently in Australia victims of cybercrime have no practical recourse available to them:

> [Lack of victim support] does nothing to reduce the sense of helplessness felt by victims of online fraud but reinforces the sense of shame and embarrassment felt by many and the isolation of succumbing to this type of offence. It also does not encourage the reporting of this type of crime to police, given that there are significant limitations on what action, if any, police can take. While the complexity of online offences presents substantial challenges to law enforcement and the criminal justice system, action needs to be taken to address this exclusion and to recognise the legitimacy of online fraud victims, in terms of the support and assistance they require as a result of what has occurred.[6]

7.10   The Committee investigated whether government could do more to encourage Internet Service Providers (ISPs) and web managers to reduce unacceptable behaviours and tolerance of criminality on their websites, including strengthening laws to ensure compliance with best practice standards and safeguards. While representatives from DBCDE told the Committee that education and awareness raising are the better means to

---

5   Telstra Corporation Ltd, *Submission 22,* p. 5.

6   Dr Cassandra Cross, *Submission 49,* p. 9.

protect seniors online, some stakeholders maintained that government could be doing more with ISPs and web managers.

7.11   The Committee was impressed by the strong and effective partnerships that have been formed to date between industry and government agencies both in Australia and overseas to raise awareness of cyber security requirements among industry players and across the broader community. The Committee notes that there is potential to build on existing engagement between government and ISPs to address cybersafety risks to seniors under the National Broadband Network.

7.12   Appropriate targeting of cybersafety messages was much discussed during the inquiry. Dr Cross presented evidence from her extensive research that cybersafety campaigns would be more successful if they targeted the risky behaviours that result in victimisation rather than focussing on the range of risks. Dr Cross explained that it is what the potential victim does when asked to send money or personal details which is crucial and the effectiveness of all prevention messages and awareness campaigns culminate in that moment. How seniors act in the moment when they are requested to transfer money or send personal details should be the focus of prevention messages about online fraud.[7]

7.13   The Committee recognises the cybersafety work of DBCDE and of the Department of Families, Housing, Community Services and Indigenous Affairs. Both host informative websites with a lot of cybersafety information, including some specifically for seniors. However, the Committee also noted that various stakeholders suggested that online cybersafety information could be more accessible and more user-friendly.

7.14   The Committee has made 13 recommendations as a result of its inquiry. These are found at the front of the report and in each relevant chapter.

7.15   In closing, the Committee would like to sincerely thank every person, organisation and department which sent a submission and/or attended a public hearing or roundtable. The Committee acknowledges with thanks the time which dozens of people contributed to this inquiry.

Senator Catryna Bilyk
Chair

7   Dr Cassandra Cross, *Submission 49,* p. 6.